Home Office

Prüm Business and Implementation Case

To assess fairly the impact on the UK, including the potential practical benefits, the potential negative impacts and the steps that would be necessary, of rejoining the Prüm Decisions (EU Council Decision 2008/615/JHA and its implementing decision, 2008/616/JHA of 23 June 2008 in conjunction with Council Framework Decision 2009/905/JHA)

November 2015

Cm 9149

Prüm Business and Implementation Case

To assess fairly the impact on the UK, including the potential practical benefits, the potential negative impacts and the steps that would be necessary, of rejoining the Prüm Decisions (EU Council Decision 2008/615/JHA and its implementing decision, 2008/616/JHA of 23 June 2008 in conjunction with Council Framework Decision 2009/905/JHA)

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

November 2015

Cm 9149

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at:

Home Office
International Criminality Unit
International Directorate
3rd Floor – Seacole Building
2 Marsham Street
London
SW1P 4DF

ICIT@homeoffice.gsi.gov.uk

Print ISBN 9781474125376
Web ISBN 9781474125383

ID 21101501 11/15 52548 19585

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

Contents

Executive Summary

The Prüm Decisions considered in this Business and Implementation Case require Member States to allow the reciprocal searching of each others' databases for:

a. DNA Profiles – required in 15 minutes.
b. Vehicle Registration Data (VRD) – required in 10 seconds.
c. Dactyloscopic Images (Fingerprints) – required in 24 hours.

In July 2013 the Government formally opted out of all police and criminal justice measures agreed before the Lisbon Treaty came into force. This included the Prüm Decisions. This took effect on 1 December 2014. That same day the Government rejoined 35 measures where it was in the national interest, and where there were clear public protection benefits in doing so. The Government did not seek to rejoin Prüm. This was because it would have been imprudent to do so when we had neither time nor money to implement it fully by 1 December and so would have opened ourselves up to the risk of infraction by the European Commission.

However, given law enforcement advice that Prüm offers the United Kingdom significant potential benefits for the investigation and prevention of crime, the Government agreed to conduct a full Business and Implementation Case and, with the agreement of other Member States, run a small Prüm-style pilot relating to the exchange of DNA profiles. It was also made clear that the final decision on whether or not to rejoin would be one for Parliament. The Business and Implementation Case has been online since 30 September and sets out the benefits that Prüm would bring to the police in the UK, how the UK would seek to implement Prüm technically and the safeguards that we would put in place should we implement Prüm. It examines the extent of exchange at the moment and looks at how this might be increased under Prüm. It looks at the cost of implementing Prüm. It also examines other Member States' usage of Prüm, looking at operational benefits, scientific safeguards and business processes.

In producing the Business and Implementation Case, the Government has worked closely with the police in England and Wales, Scotland and Northern Ireland, the National Crime Agency, Europol and Eurojust, and other Member States. We also consulted with the Biometrics Commissioner, the Information Commissioner's Office and Non-Governmental Organisations such as Liberty, Genewatch and Big Brother Watch.

Under the Prüm Decisions the initial reply is a hit/no-hit when searching against DNA profiles or fingerprints. Demographic data is not exchanged in this process. It is not possible from the information supplied with a hit for the requesting Member State, on its own, to find out the identity of the person to whom the hit refers. Following scientific verification that a 'hit' is a true one, a Member State can request the personal details of the person hit against, but there is no requirement to do so. It is at this point that demographic data is exchanged and the person against whom there has been a match is identified. Member States are also required to meet certain forensic standards.

The Prüm style pilot looked to mirror these conditions as far as possible. It took close to 2,500 DNA profiles from forces across the United Kingdom and sent them to the Netherlands, Spain, France and Germany. There were 118 hits. The number of hits, as well as evidence from those Member States already operating Prüm, strongly suggests that making the exchange of DNA profiles part of standard operating procedures will help police investigations and help to protect the public. We have had verified hits relating to a range of crimes including rape (5), sexual assault (2) and burglary (23). These hits relate to profiles provided by a wide range of police forces, including Police Scotland. The Police are actively pursuing some of the identified individuals, both inside and outside the UK. The Prüm style pilot has also allowed us to examine how we might technically implement Prüm, including the processes to follow up hits and so make implementation easier. To date, no British nationals have been the subject of a hit.

It is worth noting that UK DNA crime scene profiles have hit in one country, in two countries and even, in some cases, in three separate countries. The police have told us that the multi-country nature of the hits will prove very important in intelligence terms as these, particularly those for burglary related offences, suggest organised patterns of offending which can be the subject of a co-ordinated response.

UK police forces sent 69 DNA profiles abroad in 2014-15 using Interpol, whereas we sent 9,931 profiles in less than six months using the Prüm style pilot and would expect those numbers to be even higher if Prüm was implemented fully

It is expected that the same benefits would accrue to the UK through the exchange of fingerprints. The prime difference between sending fingerprints and DNA profiles abroad is that fingerprints operate on a quota basis (i.e. only a certain number can be sent to each Member States on a daily basis). This requires a ‘gatekeeper’ role, essentially a body to prioritise UK requests. The National Crime Agency, with its national remit, would fulfil this role, building on its existing Interpol expertise and ensuring that no individual force area would be able to prioritise its own cases over others’.

The Government recognises that some have had significant civil liberties concerns about the operation of Prüm. We would only operate Prüm with appropriate safeguards, and would put a number of these into legislation.

For example, the Government would legislate to ensure that other Member States could only search against UK held DNA profiles and fingerprints of those actually convicted of a crime. This would help to avoid innocent British citizens becoming caught up in overseas investigations. Further, to ensure consistency with our current domestic regime, we intend to limit such searches to those convicted of recordable offences only.

The Government also recognises that there is concern that the scientific quality of DNA matches that can be reported as hits under Prüm is lower than that where we would report a hit domestically. The Government would therefore legislate to ensure that we will only provide demographic details if the hit is of a scientific standard equivalent to that required to report a hit to the police domestically in the United Kingdom. The chances of such a hit being wrong are less than one in a billion. In

addition, noting the particular sensitivities around DNA profiles taken when a person was a minor we will only provide demographic detail in such cases if a formal mutual legal assistance request has been made.

All of these legislative safeguards will ensure that operating Prüm would be done in a way that respects civil liberties. Legislation will be drafted in consultation with the Scottish Government.

Prüm would also give UK police forces the ability to check the VRD of foreign registered vehicles in 10 seconds, rather than taking much longer through Interpol. This is something of particular importance to the Police Service of Northern Ireland given its land border with Ireland.

The cost estimate for delivering full Prüm implementation is £13m. This is considerably lower than the £31m estimate by the Government in 2007.

The Government has considered carefully the alternatives to Prüm, including further development of the existing exchange through Interpol. However, improving the existing cumbersome, labour intensive and slow Interpol processes is dependent on other States and Interpol. We see no likelihood of being able to make these changes. Equally, the Government does not believe it would be possible, in practice, to negotiate a bilateral agreement with the EU.

In summary, the Business and Implementation Case demonstrates that there would be undoubted operational and public protection benefits to rejoining Prüm. These would be felt across the UK. Law enforcement colleagues agree that this is the case. The Government is confident that its proposed legislative framework would allow Prüm to operate in a way that respects fully the civil liberties of British citizens. The Government therefore believes that it would be in the national interest for the UK to seek to rejoin Prüm.

Introduction

Prüm

In 2005 seven Member States[1], in the town of Prüm in Germany, signed the Prüm Treaty, recognising the need to step up cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. On 23 June 2008, significant elements of the Treaty were transposed into EU law, when the Prüm Decisions (Council Decision 2008/615/JHA, see Annex A, and Council Decision 2008/616/JHA, see Annex B) were adopted.

The Prüm Decisions have four main elements:

1. Automated search and comparison of data from national data files in the area of DNA, dactyloscopic [fingerprint] data and vehicle registration data (Chapter 2 of the Council Decision 2008/615/JHA and Chapters 2-6 of the Council Decision 2008/616/JHA);

2. Information exchange for the prevention of offences in the context of major events with a cross-border dimension and regarding possible terrorist offences (Chapter 3 and 4 of the Council Decision 2008/615/JHA);

3. Police cooperation (Chapter 5 of the Council Decision 2008/615/JHA and Chapter 6 of the Council Decision 2008/616/JHA);

4. The operational chapters are underpinned by Data Protection rules set out in Chapter 6 of Council Decision 2008/615/JHA.

In addition, the term “Prüm Decisions” should be read as including, not just the two initial decisions (2008/615 & 616/JHA) but also Council Framework Decision 2009/905/JHA(Annex C) on Accreditation of forensic service providers carrying out laboratory activities[2]. This Framework Decision requires forensic service providers (for both fingerprints and DNA) to be accredited to ISO standard 17025 and also requires Member States to treat forensic results from ISO 17025 accredited laboratories in Member States as they would a domestic ISO 17025 accredited laboratory.

The deadline to implement Chapter 2 of the two initial Decisions was 26 August 2011; however infraction proceedings were not possible before 1 December 2014. The deadline to implement the DNA accreditation provisions of 2009/905/JHA was 30 November 2013; for fingerprints it is 30 November 2015. Again no infraction proceedings were possible before 1 December 2014.

In July 2013 all three agreements were among the measures included in the block Justice and Home Affairs opt out option of pre-Lisbon criminal law and policing measures that the UK exercised in 2013. As it was not possible for the UK to

[1] The Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria
[2] Recital 7 of 2014/836/JHA (Annex D)

implement Prüm by the deadline of December 2014, rejoining in 2014 would have raised an infraction risk. Therefore Prüm was not one of the 35 measures, set out in Command Paper 8897 that the UK opted back into in 2014.

The Home Secretary stated in Parliament on 10 July 2014:

"One measure that we have successfully resisted joining is Prüm, a system that allows the police to check DNA, fingerprint and vehicle registration data. I have been clear in the House previously that we have neither the time nor the money to implement Prüm by 1 December. I have said that it will be senseless for us to rejoin it now and risk being infracted. Despite considerable pressure from the Commission and other member states, that remains the case.

All hon. Members want the most serious crimes such as rapes and murders to be solved and their perpetrators brought to justice. In some cases, that will mean the police comparing DNA or fingerprint data with those held by other European forces. Thirty per cent of those arrested in London are foreign nationals, so it is clear that that is an operational necessity. Therefore, the comparisons already happen, and must do so if we are to solve cross-border crime. I would be negligent in my duty to protect the British public if I did not consider the issue carefully."[3]

Therefore, as part of the negotiations to opt back in to the 35 measures, the Government agreed to:

Undertake a full business and implementation case to assess the merits and benefits of the UK rejoining the Prüm Decisions, in close consultation with operational partners in the UK, all other Member States, the European Commission, Europol and Eurojust; and

If the business and implementation case is positive for the UK, and following a vote in, make a decision as to whether the UK should apply to participate in the Prüm Decisions under Article 10(5) of Protocol 36 on the basis of the business and implementation case by 31 December 2015

Also on 10 July 2014 the Home Secretary said:
"... in order for the House to consider the matter carefully, the Government will produce a business and implementation case and run a small-scale pilot with all the necessary safeguards in place. We will publish that by way of a Command Paper and bring the issue back to Parliament so that it can be debated in an informed way. We are working towards doing so by the end of next year. However, the decision on whether to rejoin Prüm would be one for Parliament."

Relevant transitional and consequential measures were adopted by the Council to reflect this agreement (2014/836/EU, see Annex D, and 2014/837/EU, see Annex E) in November 2014.

[3] Hansard 10 July 2014: Column 492

Background

Context

The population of the European Union (EU) is now[4] over 500m, spread across 28 Member States. It has grown significantly over the last twelve years with A8[5] accession (74m) in 2004, A2[6] accession (29m) and with Croatia's 2013 accession (4m). The current non-UK born resident population of England and Wales is 13%[7].

The population increase and easier cross border travel is reflected in the numbers of EU nationals being arrested in the UK. Individual force arrest data[8] submitted to the ACRO Criminal Records Office (ACRO) suggests approximately 15% of all arrests nationally involve foreign nationals, this figure rises to approximately 30% for the Metropolitan Police Service (MPS) and reached as low as 2% for Durham Constabulary.

ACRO went on to develop further data from the following police forces:

Table 1 Force Arrest Data Year 2013-14[9]

Force	UK Arrests	EU Arrests	Non/EU Arrests	Total Foreign Arrests	Nationality Unknown	Total Arrests	% Foreign Nationals Arrested
Greater Manchester	**59,882**	**3272**	**3606**	**6,878**	**653**	**67,413**	**10%**
Hampshire	**31564**	**1711**	**1530**	**3241**	**-**	**34805**	**9%**
MPS	**146,231**	**33,676**	**34,498**	**68,174**	**669**	**215,074**	**31.7%**
West Midlands	**53,256**	**4272**	**4643**	**8915**	**845**	**63,016**	**14%**

Of those foreign national arrests approximately 50% are EU nationals and 50% non-EU nationals. Foreign criminality is therefore a fact of life for law enforcement agencies in the UK.

The MPS via Operation Nexus[10] has further refined the data as follows.

MPS Foreign National Offender Overview

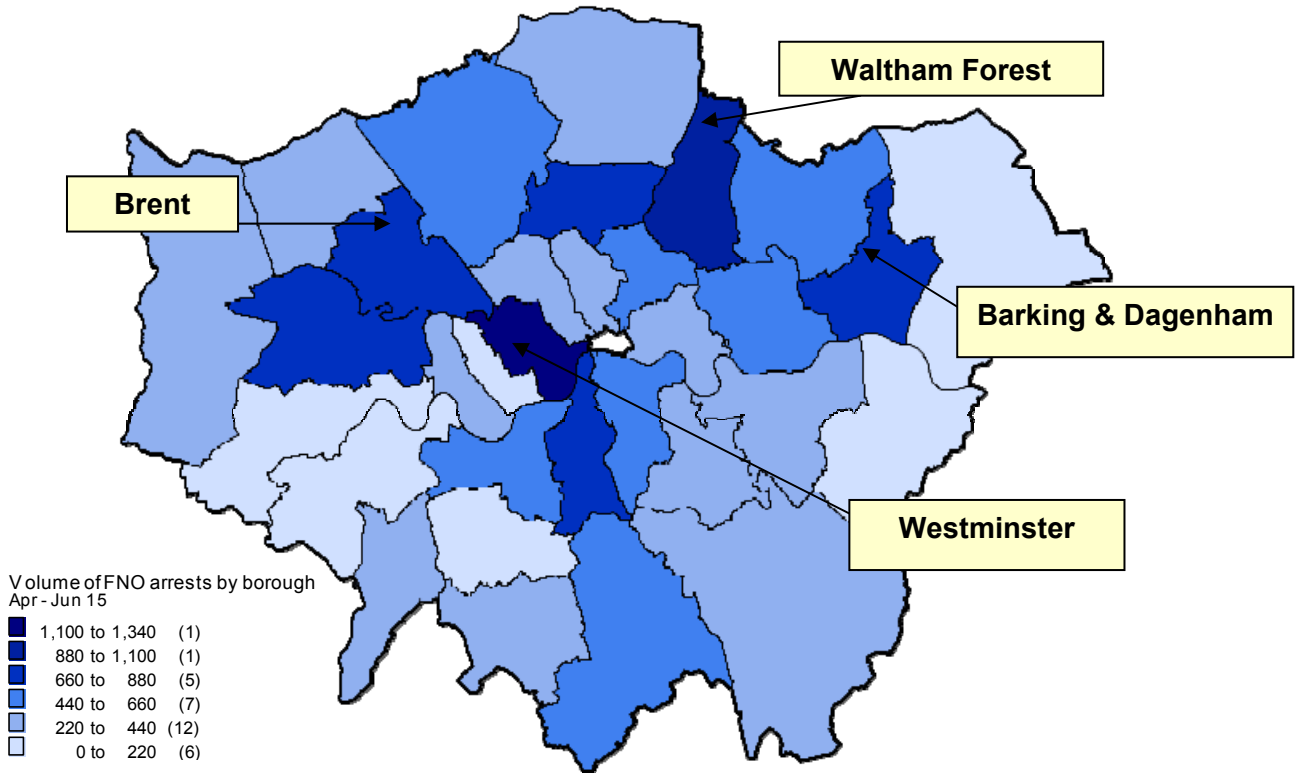
Between April and June 2015, 30% of all arrests in London were of Foreign National Offenders (FNO). Of those FNO arrests 49% were of European Foreign National

[4] http://ec.europa.eu/eurostat/statistics-explained/index.php/Population_and_population_change_statistics
[5] Estonia, Latvia, Lithuania, Poland, Hungary, Slovakia, Czech Republic, Slovenia
[6] Bulgaria, Romania
[7] http://www.ons.gov.uk/ons/rel/census/2011-census/key-statistics-for-local-authorities-in-england-and-wales/sty-non-uk-born-population.html
[8] For the financial year 2013/2014
[9] ACRO Force Arrest Data for Financial Year 2013/2014
[10] Where immigration officials work jointly with the police to boost the deportations of foreign criminals

Offenders (EU FNO). Almost a third of EU FNO arrests are made within the top 5 boroughs for EU FNO arrests.

The maps below shows the spread of all FNO and EU FNO arrests across the MPS in the second quarter of 2015

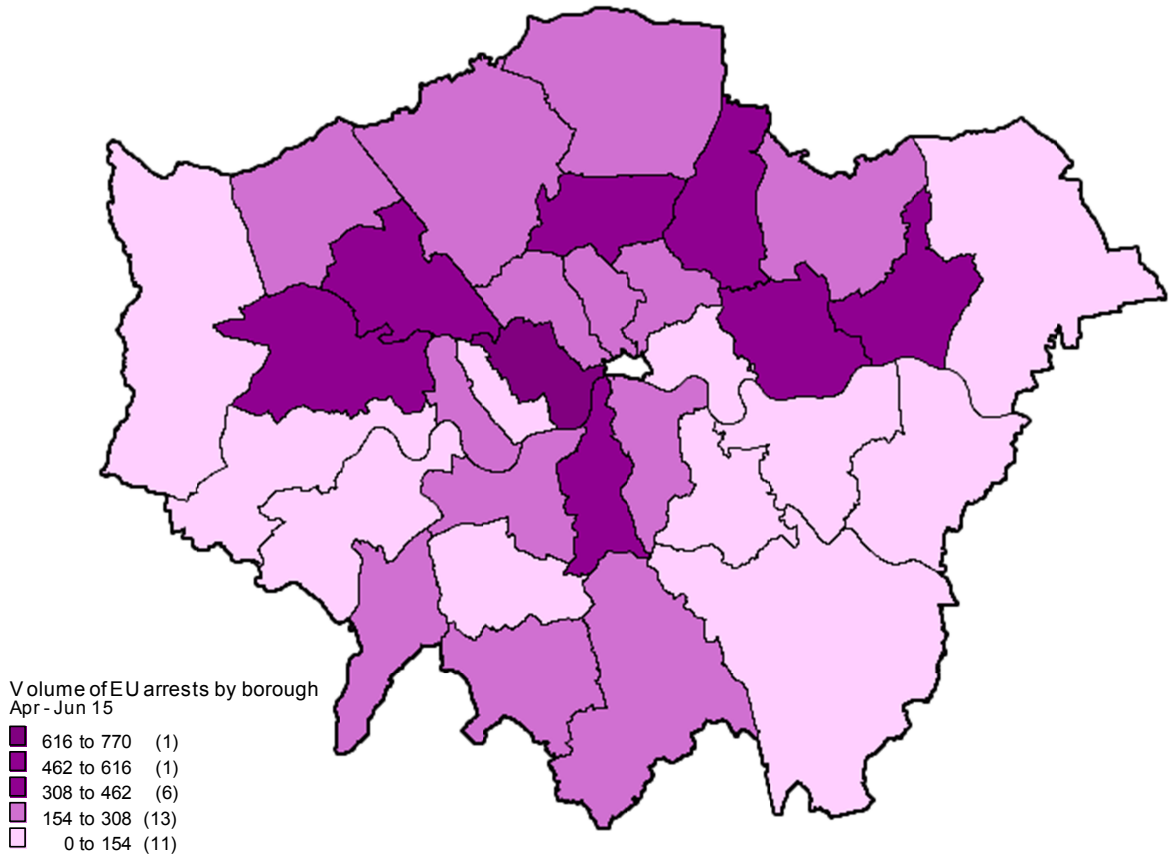
All Foreign National Offenders
(April - June 2015)



No	Borough	FNO arrests Apr-Jun 15	All arrests Apr-Jun 15	% of FNO arrests	FNO arrests Jan-Mar 15	FNO arrests Apr-Jun 14
1	Westminster	1332	3216	41%	1433	1329
2	Waltham Forest	882	2242	39%	941	825
3	Heathrow[11]	843	1985	42%	500	543
4	Barking & Dagenham	785	2176	36%	761	802
5	Brent	754	1777	42%	795	930
6	Haringey	745	1975	38%	708	705
7	Lambeth	737	2511	29%	758	716
8	Ealing	716	2019	35%	740	777
9	Newham	640	1690	38%	513	693
10	Croydon	625	2395	26%	595	569

[11] Heathrow additionally included as a borough for policing purposes.

European Foreign National Offenders
(April - June 2015)



No	Borough	EU arrests Apr-Jun 15	All arrests Apr-Jun 15	% of EU arrests	EU arrests Jan-Mar 15	EU arrests Apr-Jun 14
1	Westminster	770	3216	24%	793	760
2	Waltham Forest	470	2242	21%	533	466
3	Brent	412	1777	23%	415	511
4	Heathrow	401	1985	20%	251	238
5	Haringey	399	1975	20%	370	370
6	Barking & Dagenham	374	2176	17%	386	438
7	Lambeth	360	2511	14%	371	362
8	Ealing	344	2019	17%	329	396
9	Newham	314	1690	19%	255	362
10	Redbridge	284	1510	19%	268	283

National Searching of DNA and Fingerprints

It is possible to carry out law enforcement searches of DNA and fingerprints nationally. This is governed by various pieces of legislation. The Protection of Freedoms Act 2012[12] (PoFA) sets out rules in England and Wales for the retention of DNA profiles and fingerprints from those convicted of offences, those charged but not convicted, those arrested but not charged and those whose cases have not been concluded. The Criminal Procedure (Scotland) Act 1995 sets out rules for Scotland and the Criminal Justice (Northern Ireland) Act 2013 does the same for Northern Ireland. PoFA introduced a far stricter statutory regime for the retention and use of DNA and fingerprints and established statutory oversight of this new regime in the form of the Commissioner for the Retention and Use of Biometrics (Biometric Commissioner).

In all three jurisdictions, the law broadly allows the retention of DNA profiles[13] (as opposed to samples[14]) and fingerprints from:

- adults convicted of recordable offences,
- juveniles convicted of recordable offences (for shorter periods of time where they are first time offenders),
- those arrested, charged and not convicted of certain serious offences (but only for a limited period of time)
- those whose cases have not been concluded, for the period in which the case is being investigated/prosecuted

Otherwise, DNA profiles and fingerprints must be deleted from the national databases[15]. A DNA sample must be destroyed once a DNA profile has been derived from it, or within six months of collection, whichever is sooner. The PoFA rules, which differed from the previous England and Wales position of retaining profiles from all arrestees, led to a mass cleansing of the National DNA Database (NDNAD) and fingerprint database (known as IDENT1).

In a Written Ministerial Statement of 24 October 2013[16] Rt. Hon Lord Taylor of Holbeach and Rt. Hon James Brokenshire MP said:

"The Government have now delivered their commitment to reform the retention of DNA and fingerprint records by removing innocent people from the databases, and adding the guilty.
1,766,000 DNA profiles taken from innocent adults and children have been deleted from the national DNA database. 1,672,000 fingerprint records taken from innocent adults and children have been deleted from the national fingerprint database. ... 480,000 of the DNA profiles removed as part of this programme were taken from children."

[12] Which amended the Police and Criminal Evidence Act 1984
[13] Any information derived from a DNA sample
[14] Any material that has come from a human body and consists of or includes human cells
[15] There are a few exceptions for this, for example in relation to biometrics taken under terrorism powers, material which may become disclosable under the Criminal Procedure and Investigations Act 1996 and material subject to a national security determination
[16] http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131024/wmstext/131024m0001.htm

The Biometric Commissioner's Annual Report 2014[17] found that overall the relevant provisions of the Protection of Freedoms Act 2012 had been properly implemented and that there is effective regulation of the retention and use by the police and other law enforcement authorities of DNA (samples and profiles) and fingerprints.

International Searching

Current international criminal investigation data exchange for the UK for DNA, fingerprints and vehicles is facilitated manually through the National Crime Agency (NCA) UK International Crime Bureau (UKICB)[18] utilising agreed exchange mechanisms via Interpol. The volume of transactions is limited by the availability of resources both within the NCA and UK data processers. Interpol exchange channels and processes are often seen as cumbersome and untimely.

[17] https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2013-2014

[18] Separately, criminal records are transferred via the European Criminal Records Information System (ECRIS) by ACRO. The MPS cover counter terrorism matters.

Options

The business and implementation case will focus on the following three options:

1. **Do Nothing, maintain the status quo -** Information requests between the UK and Member States using Interpol channels continue for DNA profiles, fingerprints, vehicles and vehicle keeper information

2. **Fully Implement Prüm -** Develop and deploy full outbound and inbound Prüm infrastructure to enable Member States and UK to access each other's databases for DNA profiles, fingerprints and vehicle registration data to combat terrorism and cross border crime. This option can also be delivered as a phased or deferred option. This would defer some expenditure and allow for the introduction of Prüm requirements into the new strategic solutions for fingerprints and DNA profiles which are planned for the next few years.

3. **Alternatives to Prüm -** In addition to running existing systems as set out in Option 1; develop enhanced bilateral arrangements with other Member States in relation to information requests for DNA profiles, fingerprints and vehicle keeper information.

These options are explored in more detail below.

Option 1: Do Nothing/Maintain the Status Quo

Description of Option

Current legislation[19] allows for the international sharing of fingerprints, DNA profiles and vehicle registration data for the prevention, detection, investigation or prosecution of crime. The sharing of the data must be necessary for that purpose. Any data shared must be relevant and not excessive, must be accurate and up to date, and there must be in place appropriate technological and organisational measures against unauthorised or unlawful processing and against accidental loss or destruction or personal damage.

Option 1 would mean information requests between the UK and Member States would continue using existing channels for DNA profiles, fingerprints, vehicles and vehicle keeper information.

International criminal investigation data exchange for the UK for DNA, fingerprints and vehicles is currently facilitated manually through the National Crime Agency (NCA).[20]

Requirements

- Information requests between the UK and Member States using Interpol channels continue for DNA profiles, fingerprints, vehicles and vehicle keeper information.
- All inbound requests prioritised according to seriousness, urgency and capacity to respond.
- NCA continue to manage urgent information exchanges concerning serious crimes using Council Framework Decision 2006/960/JHA.
- Do not develop a UK Prüm solution.

Current Interpol Process

For the detailed process map, please see Annex F. The high level incoming process is as follows:

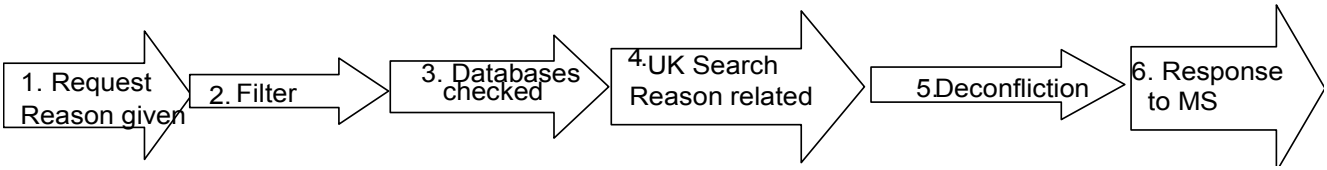


Figure 1 current Interpol process

[19] Police And Criminal Evidence Act 1984 (as amended), Police and Criminal Evidence (Northern Ireland) Order 1989 (as amended) and Criminal Procedure (Scotland) Act 1995

[20] Separately ACRO operates the European Criminal Record Information System (ECRIS) which enables the exchange of criminal conviction information between EU Member States. The MPS cover counter terrorism matters.

At steps 1 and 2 the inbound requests are sorted by the reason for a request and the nature of the request before allocation.

At step 3 NCA will attempt to search a number of policing databases (such as the Police National Computer) to determine if the person (if personal details are provided) or vehicle is already known and recorded.

At step 4 the relevant agencies search the NDNAD and IDENT1 to determine if a DNA or fingerprint match exists and respond to NCA with the results.

At Step 5 if a match is found against the request NCA will carry out a risk assessment to ensure that it is safe to share the information.

At step 6 NCA responds to the requesting country.

The NCA's procedures regarding inbound and outbound requests are currently managed by the NCA's UK ICB. There is a small team of five officers in the UKICB which has in-depth knowledge of biometric exchanges.

Data Available for Exchange

DNA and Fingerprints

In the post PoFA regime UK crime scene DNA profiles and latent fingerprint marks are searched against all legitimately retained information, i.e. conviction and non-conviction profiles/prints. This also happens under the Scottish system which was the model for the regime set out in PoFA. In addition, Parliament has specifically provided for a legitimately retained profile to be used in the investigation of crime abroad[21].

England and Wales[22]

Convictions

Situation	Fingerprint and DNA Retention
Any age convicted (including given a caution or youth caution) of a qualifying[23] offence	Indefinite
Adult convicted (including given a caution) of a recordable[24] offence	Indefinite

[21] Police and Criminal Evidence Act 1984 63(A) (when read with the retention rules set out in the Protection of Freedoms Act) and Criminal Procedure (Scotland) Act 1995 s19C. Within NI Police Criminal Evidence (Northern Ireland) Order 1989 s63 (when read with the retention rules set out in the Protection of Freedoms Act and Criminal Justice Act 2013)

[22] This table does not include the Terrorism Act 2000 retention periods.

[23] A 'qualifying' offence is one listed under section 65A of the Police and Criminal Evidence Act 1984 (the list comprises sexual, violent, terrorism and burglary offences).

[24] A 'recordable' offence is one for which the police are required to keep a record. Generally speaking, these are imprisonable offences; however, it also includes a number of non-imprisonable offences such as begging and taxi

Situation	Fingerprint and DNA Retention
Under 18 convicted (including given a youth caution) of a recordable offence (which is not a qualifying offence)	1st conviction: 5 years (plus length of any prison sentence), or indefinite if the prison sentence is for 5 years or more. 2nd conviction: indefinite

Non-convictions

Situation	Fingerprint and DNA Retention
Any age charged with but not convicted of a qualifying offence	3 years plus a 2 year extension if granted by a District Judge (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded[25])
Any age arrested for but not charged with a qualifying offence	3 years if granted by the Biometrics Commissioner plus a 2 year extension if granted by a District Judge (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Any age arrested and subject to a National Security Determination	2 year extension on first and any subsequent determination
Any age arrested for or charged with a recordable offence (which is not a qualifying offence)	None (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Adult given a Penalty Notice for Disorder	2 years
Any age arrested for recordable offence – case not concluded	Until case is concluded

Scotland[26]

Convictions

Situation	Fingerprint and DNA Retention
Person[27] convicted of an offence	Indefinite

touting. The police are not able to take or retain the DNA or fingerprints of an individual who is arrested for an offence which is not recordable.

[25] An 'Excluded' offence is a recordable offence which is minor, was committed when the individual was under 18, for which they received a sentence of fewer than 5 years imprisonment and is the only recordable offence for which the person has been convicted.

[26] Retention rules are set out in Part 2 of the Criminal Procedure (Scotland) Act 1995. Section 18(3) outlines a general rule of destruction of samples following a decision not to institute criminal proceedings or when proceedings do not end with conviction, exceptions to the general rule are found within sections 18A to 18G of the 1995 Act.

[27] This may (rarely) include children. Part 5 of the 1995 Act deals with the criminal justice treatment of children and young people. The age of criminal responsibility in Scotland is 8 (section 41) though no child under 12 may be prosecuted (section 41A) and children under 16 may only be prosecuted on the instruction of the Lord Advocate (section 42). In practice children under 16 are not usually prosecuted and offending behaviour is dealt with instead by way of referral to the children's hearing system.

Non-convictions

Situation	Fingerprint and DNA Retention
Person subject to criminal proceedings for relevant sexual or violent offence[28]	3 years following conclusion of proceedings, plus a 2 year extension(s) if granted by a Sheriff[29]
Person offered an alternative to prosecution[30] for an offence that is not a relevant sexual or violent offence	2 years plus a 2 year extension(s) if granted by a Sheriff[31]
Person offered alternative to prosecution for an offence that is a relevant sexual offence or violent offence.[32]	3 years plus a 2 year extension(s) if granted by a Sheriff[33]
Person arrested and subject to a national security determination	2 years and may be renewed by any subsequent determination[34]
Person subject to certain fixed penalty notices[35]	2 years[36]
Child referred to a children's hearing on grounds of having committed a relevant sexual or violent offence[37]	3 years[38], with two year extensions if granted by a Sheriff[39]

Northern Ireland[40]

Convictions

Situation	Fingerprint and DNA Retention
Any age convicted (including given a caution or youth caution) of a qualifying offence	Indefinite
Adult convicted (including given a caution) of a recordable offence	Indefinite
Under 18 convicted (including given	1st conviction: 5 years (plus length of any

[28] These terms are defined in section 19A (6) of the 1995 Act.
[29] Section 18A of the 1995 Act.
[30] Prosecutors may offer a fixed penalty, compensation offer or work order – see sections 302 to 303ZB of the 1995 Act.
[31] Section 18B of the 1995 Act.
[32] The list of relevant sexual and relevant violent offences is set out in section 19A (6) of the 1995 Act.
[33] Section 18C of the 1995 Act.
[34] Section 18G of the Criminal Procedure (Scotland) Act 1995.
[35] This covers fixed penalty notices issued by a police constable under section 129 of the Antisocial Behaviour (Scotland) Act 2004 for antisocial behaviour offences relating to drunkenness, vandalism, breach of the peace, etc.
[36] Section 18D of the 1995 Act.
[37] For the purposes of section 18E of the 1995 Act, the relevant sexual or violent offences are set out in a statutory instrument, the Retention of Samples etc. (Children's Hearings) (Scotland) Order 2011 (SSI 2011/197).
[38] Section 18E of the 1995 Act.
[39] Section 18F of the 1995 Act.
[40] At the time of writing the Northern Ireland retention rules in Schedule 2 of the Criminal Justice Act (Northern Ireland) have yet to be commenced.

Situation	Fingerprint and DNA Retention
a youth caution) of a recordable offence (which is not a qualifying offence)	prison sentence), or indefinite if the prison sentence is for 5 years or more. 2nd conviction: indefinite

Non-convictions

Situation	Fingerprint and DNA Retention
Any age charged with but not convicted of a qualifying offence	3 years plus a 2 year extension if granted by a District Judge (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Any age arrested for but not charged with a qualifying offence	None[41]
Any age arrested and subject to a National Security Determination	2 year extension on first and any subsequent determination.
Any age arrested for or charged with a recordable offence (which is not a qualifying offence)	None (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Adult given a Penalty Notice for Disorder	2 years
Any age arrested and DNA/FP taken but case not concluded	Until case is concluded

In addition all data held by the Driving and Vehicle Licensing Agency (DVLA) on vehicles and vehicle keepers can be searched by NCA via the PNC as part of an Interpol request.

Vehicle Registration Data

The police in England, Scotland, Wales and Northern Ireland, have direct access to vehicle registration data ((VRD) vehicle keeper; previous keepers; vehicle details, including sold and not re-registered; insurance; MOT) via the PNC on UK registered vehicles. This information can be accessed in one of four ways: by calling a control centre; using a mobile data terminal; using operational blackberry devices or using radio communications. Some road policing vehicles are fitted with a computer terminal which provides limited access to PNC. The immediate access to VRD allows the appropriate level of investigation to take place whilst a driver remains with the enquiry officers, supports officer safety and public protection. The VRD is received from the DVLA. The PNC holds information on convictions, stolen vehicles

[41] [1] Article 63D(5)(c), 63D(11) to (13) and the definition of prescribed in Article 63D(14) of PACE NI make provision for material from persons arrested but not charged with a qualifying offence to be retained for 3 years if granted by the NI Biometric Commissioner plus a further 2 years if granted by a District Judge. At the time of writing these provisions have not been commenced and are unlikely to be for the foreseeable future.

or vehicles known to have been involved in crime. Information previously held by the Driver and Vehicle Agency (DVA) in Northern Ireland was, from 21 July 2014, transferred to the DVLA in Swansea.

UK police officers are not able to routinely obtain keeper details of foreign registered vehicles using UK roads. Police have told us that this is a significant hindrance. There is particular concern in Northern Ireland as they share a land border with a Member State yet the Police Service Northern Ireland (PSNI) has no routine access to Irish VRD data. The PSNI access data on EU registered vehicles via the Extradition and International Mutual Assistance Office (EIMA). Generally speaking, however, the information is not available for foreign cars. Lack of data and delays in accessing information cause delays with investigations.

UK police operations

There are hundreds of thousands of foreign registered vehicles on UK roads at any time. UK police have concentrated their efforts into conducting operations focusing on foreign registered vehicles using UK roads. In Operation Trivium 3, officers from fourteen EU countries worked with British police officers from a control centre in the West Midlands. The foreign officers helped British officers overcome language obstacles and were also able to use their home country's police intelligence systems to access the VRD to verify details supplied by foreign nationals who were being questioned. This instant access to VRD held on foreign systems was extremely useful to British policing and a very effective method of targeting foreign criminals using the UK road network as a means of furthering their crimes. Operation Trivium 4 took place in June 2015 and the results will be published soon.

Cross Border Enforcement Directive

The Government is required to allow Member States to access vehicle keeper details held in the UK so as to implement a new Directive on Cross Border Enforcement (CBE) 2015/413/EU[42] of road safety traffic offences. As a minimum this must allow incoming requests, from Member States, for the vehicle keeper details of British registered vehicles, by May 2017. This will take place through EUCARIS (the European Car and Driving License Information System)[43].

Information will be exchanged in real-time or by batch. The road traffic offences covered are:

- speeding;
- failure to stop at a red light;
- use of a forbidden lane;
- drink driving;
- drug driving;
- failure to wear a seat belt;
- failure to wear a safety helmet; and,
- use of a mobile phone or other communications device when driving

[42] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0413
[43] EUCARIS is an information exchange system that provides an infrastructure and software to countries to share VRD

Other Exchanges

UK law enforcement agencies can currently use a range of methods through Interpol and via EU measures to exchange non-personal data and provide assistance internationally. In addition the UK provides much of the information set out in Chapters 3 to 5 the Prüm Decisions. These powers also allow the UK to share information with other Member States for the prevention and detection of crime, subject to the overall requirements of the Data Protection Act and the Human Rights Act.

Volumes

The volume of transactions currently processed by the NCA is limited by the availability of resource both within Interpol, NCA and the UK data processers. Requests for information, particularly on DNA and fingerprints, are often an integral part of a much more complex request and are not easily separated. Requests for searches of vehicle registration data are not separately reported by the NCA. However, it is known that the volumes of requests both incoming and outgoing via this route are low. The Biometric Commissioner's Annual Report 2014[44] listed the following volumes of transactions:

Table 2 NCA Transactions

Type of transaction	Per month
DNA subject profiles received from other countries	2
DNA crime scene profiles sent to other countries	4
DNA crime scene profiles received from other countries	30
Fingerprint requests sent to other countries	75
Fingerprint requests received from other countries	4
Finger mark requests from other countries	2
Finger mark requests send to other countries	>1

In addition he noted that between January 2013 and September 2014 only 9 DNA subject profiles were sent abroad.

[44] https://www.gov.uk/government/publications/biometrics-commissioner-annual-report-2013-2014

Table 3 MPS Case studies searching biometrics abroad and highlight the extended timescales involved using current searching facilities

Country	Details
UK	A request to search DNA from a linked series of 13 burglaries in and around London was sent via Interpol in July 2014. Germany sent intelligence of a potential match on the Spanish databases in September 2014. This match was confirmed and the details of a Romanian national released in January 2015. At this point it was found that the suspect had been arrested a week before by Essex police and was on bail. A warrant was circulated for his arrest.
UK	In October 2014 a victim was raped by an unknown stranger 'Polish or Romanian' as she walked home. A search of DNA on the European databases via Interpol in December 2014 revealed a match of a Romanian national on the Romanian database at the end of January 2015. A warrant has been circulated for his arrest and potential links to a further case of outraging public decency are to be investigated.
UK	At the end of January 2015, MPS were informed about a rape by a male believed to be Romanian. It was a sustained sexual attack that lasted 90 minutes. DNA was searched on European databases via Interpol and a match was reported from the Romanian database a month following request. The suspect was arrested a week before the DNA results came through and was charged for the above offence. The defendant pleaded guilty to rape and two counts of assault by penetration on August 2015. He is to be sentenced in September. The defendant has previous convictions in Romania for Robbery and murder; details of these have been requested for sentencing.
Netherlands	Three suspects were arrested for a murder in the Netherlands 2015. Forensic results indicate a potential two further suspects remained unidentified. When interviewing a suspect in custody they stated that one of the unidentified suspects may be known to the UK databases under a different name. An Interpol search was conducted on the UK databases in June 2015 and this matched with a UK, MPS subject. Following a series of checks the UK were able to supply details of the Albanian passport which was seized upon his arrest in the UK for Possession with intent, his PNC name and a photograph. A SIRENE alert was circulated.
UK	A disk of 164 finger marks submitted to Romania for speculative search in November 2012. This resulted in a hit of evidence from an MPS burglary scene against a Romanian national in March 2013. The suspect was charged and remanded to attend court in January 2014. Found guilty, the suspect was sentenced to community order and fines in January 2014.

UK	Following an armed robbery in jewelers in Central London in 2014 intelligence suggested possibly other offences across Europe. A full DNA profile from blood generated a scene to scene match with an offence in Germany and identified a Lithuanian male. The suspect is currently circulated as wanted.

Requests for searches of vehicle registration data are not separately reported by the NCA. However, the first results for Operation Trivium 3, which utilised VRD from Member States, led to the following outcomes:

Table 4 Operation Trivium 3: October 2014 Results[45]

Result	Volume
Vehicles stopped	7000+
Vehicles seized	500+
People encountered	10000+
Arrests	1000+
Enforcement actions	3000+

Benefits

No additional funding required for implementation or downstream costs.

The UK would not be required to cede further jurisdiction on these matters to the European Court of Justice.

The risk of releasing the demographics of an innocent person as a result of a DNA and fingerprint matches remains low as a result of the Protection of Freedom Act 2012 changes to retention.

Risk

The current international exchange channels and processes are often poorly defined and cumbersome [Annex G]**.** In addition Interpol requests are risk assessed after submission. The NCA's UKICB encourage early engagement with them to ensure any requests are actioned as quickly as possible, but failure by the investigating officer to supply all the relevant information for the risk assessment can result in a request being rejected. This leads to inconsistent submission choices across similar cases and low levels of transactions which seem counter intuitive given what is known about cross border crime. However, even with resources and will, the UK would be unlikely to change the current length of the Interpol process or the format of the universal request form as it is a worldwide resource subject to the demands of 190 member countries[46].

[45] https://www.tispol.org/news/articles/operation-trivium-3-brings-excellent-results-across-england-and-wales

[46] http://www.interpol.int/Member-countries/World

Current Interpol processes do not require a timed response. This means that the UK is potentially missing opportunities to promptly identify and apprehend foreign nationals who are committing offences or reoffending.

Table 5 Snapshot of Interpol DNA search requests made from the Metropolitan Police Service 2011-2015[47]

Number of cases recorded	**54**
Number of cases with results	**22**
Number of results recorded / Number of requests	**41%**
Average number of days taken for DNA request to be forwarded to NCA	**8 days**
Average number of days for result to come back	**143 days**
Days for responses ranged between 5 and 671 with large ranges even within countries. At the moment there is no clear pattern for those who respond quickly or not.	

There would remain no effective mechanism for routine bulk exchange of international information on volume crime.

During the lifetime of the Prüm Pilot (see Option 2) the UK agreed to attempt a bulk exchange of 250 DNA profiles using existing channels and processes with the Netherlands. This proved very difficult to arrange legally. While it is possible to exchange profiles through Interpol, Dutch law requires a request to be made by a Prosecutor, as opposed to through police to police channels. In addition exchange through Interpol is designed around a one-off process, with manual transcription of DNA profiles. Sending 250 profiles would have required transcribing each one individually. It was decided that this was too resource intensive to proceed. This exercise highlighted the legal and practical difficulties of existing processes. We

Opportunities to reveal crime trends and patterns are missed as there would be no identification of offending patterns across Member States.

[47] data collated from requests made through MPS DNA unit only

Other Existing NCA/Interpol Methods

International DNA Search through MoU Agreement with G8 Countries

The International G8 DNA Search Agreement was established to secure a way to send crime scene profiles directly between database units for checking against DNA databases with other G8 countries and uses the Interpol Search Request Network (SRN). The current members with agreements are the United Kingdom, the USA, and Canada. Australia is due to join. The agreements will allow UK forces to search their unsolved serious crime scene profiles against approximately 20 million subject profiles in three continents.

Under the terms of the governing Memorandum of Understanding the network will only be used to search single source profiles from serious unsolved crime scenes. The profiles sent can only be used in the investigation, detection and/or prosecution of crime and may not be retained by the requested country. The requested country will return a hit/no hit/not searched response to the requesting country as quickly as possible. In reality, this tends to be within two working days. Any follow-up work required as a result of a hit will be carried out via the usual Mutual Legal Assistance (MLA) processes.

Any country retains the right to refuse a search request if they do not feel it is appropriate for whatever reason. They are not obliged to give that reason, merely to report that the profile has not been searched

It uses the Interpol secure I24/7 network to send DNA profiles from one country's database to another country's database. This allows the technical experts to converse directly and flush out any problems with the profile to be searched.

However since the system went live, only the following searches have taken place:

UK - US searches - 13 (0 matches)

US - UK searches - 8 (0 matches)

There have been continued difficulties with the robustness of the IT network communications.

Interpol's DNA database

Known as the DNA Gateway, the database was initiated in 2002; by the end of 2013 it contained more than 140,000 DNA profiles contributed by 69 member countries. Participating countries use the DNA Gateway as a tool in their criminal investigations, and it detects potential links between DNA profiles submitted by member countries. Member countries can access the database via the organization's I-24/7 global police communications system and, upon request, access can be extended beyond the member countries' National Central Bureaus to forensic centres and laboratories

On the Interpol DNA Database a number of unidentified person profiles were held. In line with the UK and Interpol policy a review is required every 5 years. These profiles were recently reviewed by the NCA's UKICB.

As a result of a dip sample, a decision was made by the UKICB to remove the all the UK DNA profiles held on the Interpol Database for reviews to be undertaken. Police Forces and other Law Enforcement Agencies are currently reviewing these profiles. Once this has been undertaken relevant profiles will be resubmitted for inclusion on the Interpol Database. The NDNAD have written to all force forensic managers asking them to review the profiles and to re-submit to UKICB for uploading.

Option 2: Fully Implement Prüm Decisions[48]

Description of Option

Develop and deploy full outbound and inbound Prüm infrastructure to enable Member States and UK to access each others databases for DNA, fingerprints and vehicle registration data to combat terrorism and cross border crime. For fingerprint and DNA searches, direct access would only be available for searching for a 'hit /no hit' response initially, with safeguarded follow up activity for release of personal information. This option can also be offered phased or deferred. This would defer some expenditure and allow for the longer term introduction of requirements into the new tenders for the fingerprint and DNA infrastructure contracts.

Chapters 3-5

This business case focuses on Chapter 2 of 2008/615/JHA and Framework Decision 2009/905/JHA. Should the UK rejoin Prüm we would also have to meet the obligations set out in Chapter 3 to 5 of Prüm.

Chapter 3 of Prüm concerns the provision of non-personal and personal information between Member States to prevent criminal offences and maintain public order in connection with cross border public events (for example European Council meetings and sporting events). In Article 13 Member States are required, both spontaneously and on request, to provide non personal data concerning these events. In Article 14 they are required to provide, again both spontaneously and on request, personal data concerning those who are expected to commit criminal offences or pose a threat to public order and security at those events. Member States are also required to provide a national contact point for such exchanges.

The UK already provides personal and non-personal data concerning people who are believed to be travelling from the UK to attend and disrupt major events, for example football championships[49]. The UK will therefore not need to change its current practice in order to comply with Articles 13 and 14.

Chapter 4 of Prüm concerns the provision of personal information between Member States to prevent terrorist offences. Article 3(1) specifically allows Member States to provide information even without being requested to do so. The information sharing part of Chapter 4 is permissive – the UK does not have to provide information. The UK has mechanisms in place for sharing information relating to countering terrorism with international partners.

[48] EU Council Decision 2008/615/JHA (Chapter 2) and its implementing decision, 2008/616/JHA of 23 June 2008 (in conjunction with Council Framework Decision 2009/905/JHA) are commonly referred to as the Prüm Decisions.
[49] See Option 1

Chapter 5 of Prüm concerns “other forms of co-operation”. Article 17 concerns joint patrols and other joint operations. It is a permissive clause – i.e. it does not require such co-operation but rather allows it. If there is an agreement to co-operate, Member States may confer executive powers on the seconding Member State’s officers. In individual cases and if national law permits officers in another country are permitted to be armed.

Article 18 concerns a duty to provide mutual assistance in connection with mass gatherings, similar major events, disasters and serious accidents with a cross border element. Member States are required to notify each other in the event of such a happening, to take necessary policing measures within their territory and are permitted, on request, to dispatch officers, specialists and advisers to assist the other Member State.

While the UK would not use the powers allowed in Article 17 and 18 to run Joint Investigation Teams (it uses the powers in Framework Decision 2002/465/JHA), and would never use Prüm to permit foreign officers to carry firearms in the UK, there may be value in using Articles 17 and 18, and the ability to wear protective equipment in Article 19, to allow UK officers deployed overseas in connection with football matches to wear protective equipment to increase their personal safety. Such officers at present do not wear protective equipment.

Chapter 2

Chapter 2 provides a mechanism for the international exchange of DNA, Dactyloscopic (i.e. fingerprints), and vehicle registration data by Member State police and law enforcement agencies to combat terrorism and cross-border crime.

The Prüm Decisions enable Member States to search other Member States fingerprints and DNA databases via an automated system, on a hit/no hit basis, or directly into vehicle registration databases within the following mandatory response times:

- DNA – 15 minutes
- Fingerprints – 24 hours
- Vehicles – 10 seconds

Where matches are identified, existing secure police or mutual legal assistance channels can be used to request further (personal) information in accordance with well-established and safeguarded procedures.

The underlying end-to-end business processes and information exchanges between the UK and Member States referred to in the Prüm Decision already exist and are therefore “business as usual”.

The Prüm Decisions automate the front end of the existing system for DNA and fingerprint checking between Member States with the intention of streamlining the business process, introducing new standards for information exchange and improving access to information.

Framework Decision 2009/905/JHA

Council Framework Decision 2009/905/JHA on accreditation of forensic service providers carrying out laboratory activities requires, in Article 4, forensic service providers carrying our laboratory activities (for both fingerprints and DNA) to be accredited by a national accreditation body as complying with EN ISO/IEC 17025. In Article 5 it requires the results of ISO 17025 accredited forensic service providers in other Member States to be treated as being equally reliable as similarly accredited forensic results from domestic laboratories. Article 5(2) states that these rules do not affect national rules on the judicial assessment of evidence, i.e. court proceedings.

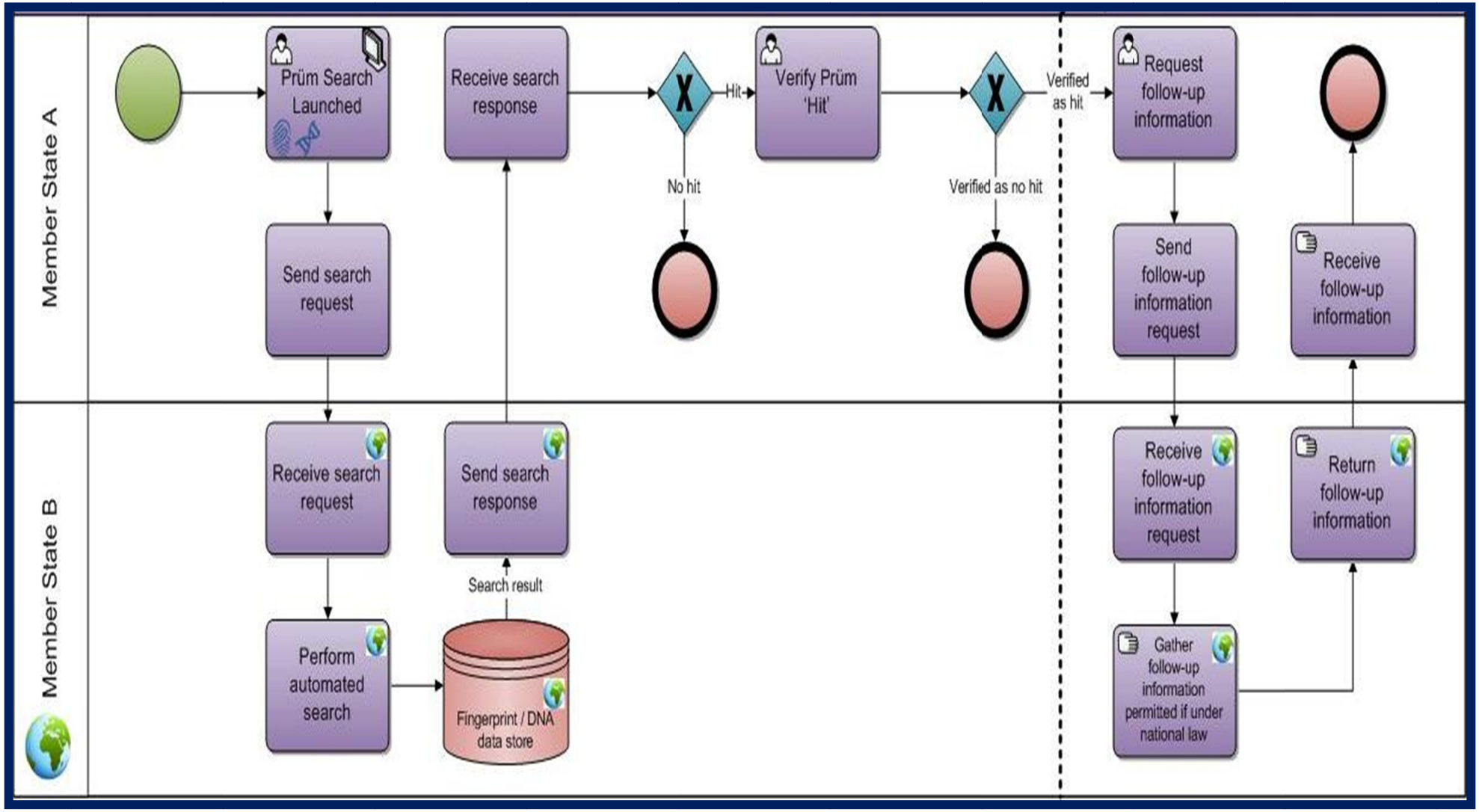


Figure 2. Outline of the Prüm Fingerprint and DNA search process.

The Prüm Decisions fully automate vehicle data exchanges between Member States against certain mandatory statutory criteria, there are also some optional criteria.

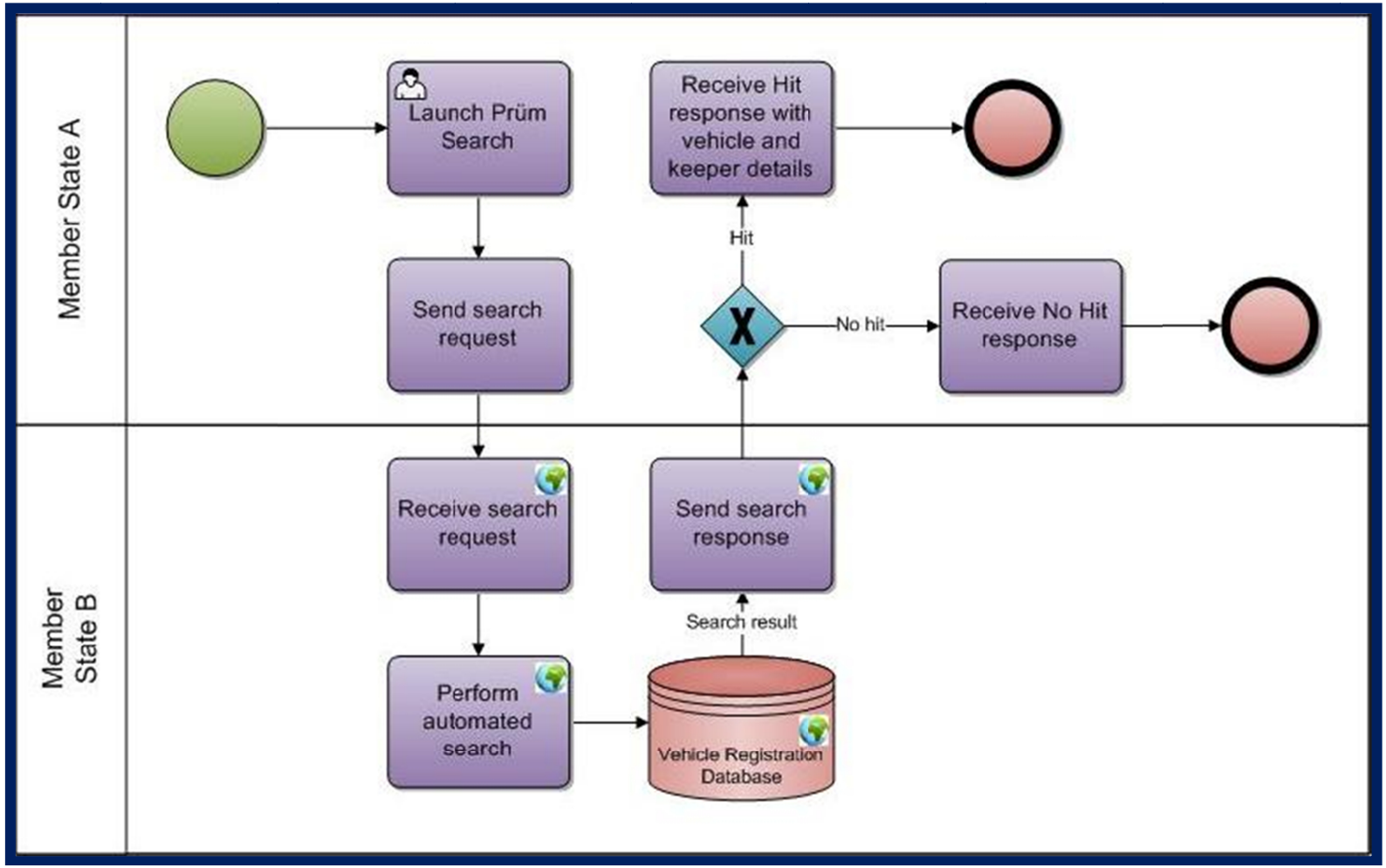


Figure 3. Outline of the Prüm vehicle registration data search process.

The very high level process model illustrated in Figure 2 and 3 and detailed below in Figure 4 compares the existing business process[50] for an inbound DNA and fingerprint information request to the UK before the changes required by Prüm and after the implementation of a Prüm option. In the diagram below, white steps are manual processes and the yellow ones indicate where a Prüm solution requires automation. The diagram shows how Prüm would partially automate DNA and fingerprint queries. Vehicle queries would receive an end-to-end automated response.

NCA/Interpol As Is[51] & Potential Prüm Business Processes (High Level)

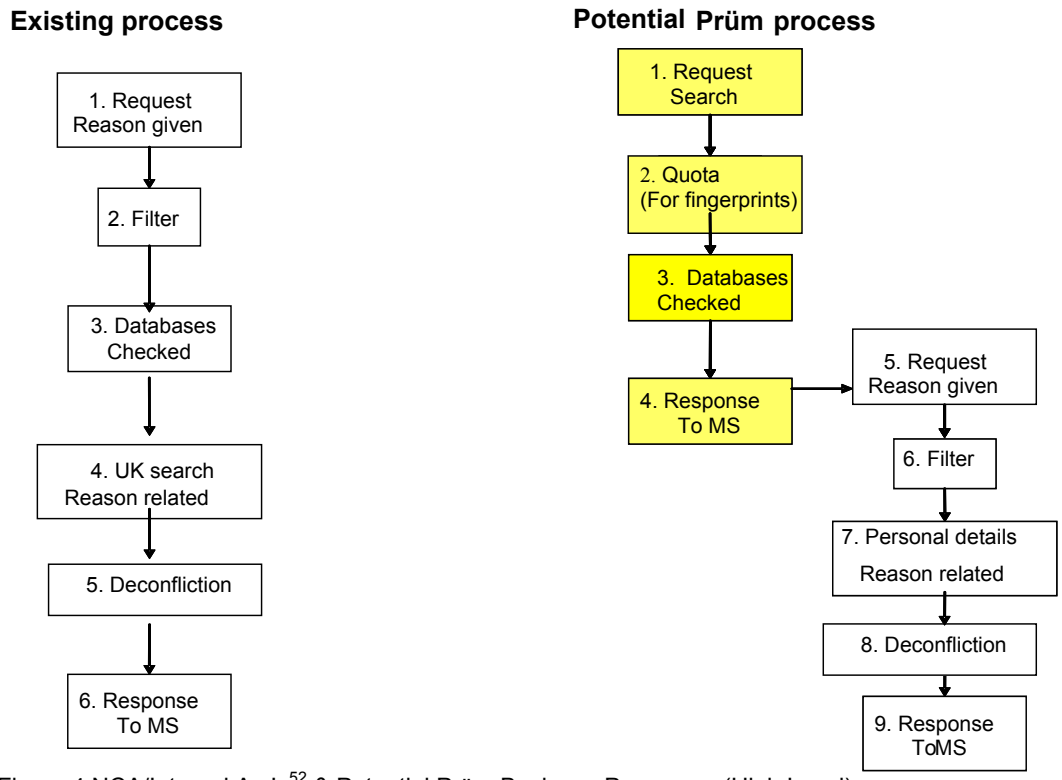


Figure 4 NCA/Interpol As Is[52] & Potential Prüm Business Processes (High Level)

Potential Prüm Business Process

The future Prüm business process shown above automates aspects of the existing process. At step 1 a Member State can search in an automated fashion and anonymised version of the UK's datasets via a secure EU network and can initiate a request without giving a reason for the request.

The volume of requests for fingerprints is controlled by a quota system at step 2; this could be a manual or automated process for the UK.

The new database approach at step 3 automates the search for data held on UK databases to see if a match or no match response can be obtained. An automated

[50] Described in detail in Option1
[51] Reference Option 1 section above
[52] Reference Option 1 section above

response reporting a “Match” or “No match” is sent to the requesting Member State within the mandatory response times[53]:

In the case of a DNA or fingerprint match, the requesting State must follow the existing manual business process for mutual assistance and request the relevant personal data related to the reason for the request through existing channels. Steps 5 to step 9 follow the existing business process.

A successful vehicle query will see all the relevant UK-held data (as set out in the Prüm Council Decision) returned to the requesting state automatically via the EUCARIS.

At its core, Prüm potentially provides the strategic platform that could assist the UK authorities in separating out and identifying criminals from law abiding migrants and travellers. It could help greatly with suspect identification/elimination and investigation.

The UK’s database infrastructure has changed since the UK initially had to consider whether to implement the Prüm Decisions. Consideration was given to whether the UK should implement the Prüm Decisions in the Gartner Scoping Study, October 2008 - March 2009. At that time there were significant and expensive barriers to the UK's ability to join Prüm. Since then:

- Regional variations in Northern Ireland in relation to fingerprints have been removed as Northern Ireland is now linked to IDENT1 and PNC.

- The Northern Ireland DVA vehicle records have been fully integrated with DVLA complying with the Prüm Decision requiring each participating country to provide a single consolidated database for searching against.

- IDENT1 and the NDNAD have been cleansed following the implementation of the Protection of Freedoms Act 2012, with c1.7 million DNA profiles and fingerprint sets being deleted.

Pilot

The business and implementation case includes evidence from a small scale pilot exchange of DNA profiles with four of the Member States currently applying Prüm namely The Netherlands, Spain, France and Germany. The main objective of the pilot was to test, within a tightly controlled environment, how Prüm style bulk exchanges of data would work in practice, providing valuable insights into both the technical and operational requirements of such exchanges as well as the number of hits that could potentially be generated by Prüm in the field of DNA.

To enable the delivery of the pilot, whilst being cognisant of civil liberty concerns regarding Prüm, arrangements with each Member State were underpinned by stringent safeguards to protect personal data. These are set out in more detail below

[53] DNA – 15 minutes, fingerprints – 24 hours, vehicles – 10 seconds

but incorporate both the data protection requirements set out in the Prüm Council Decision whilst adding further measures, such as exchanging only profiles from crimes where there is a high potential evidential value; limiting the size of the available UK data-set; and by ensuring that all profiles exchanged were of a high quality standard (which was higher than the minimum standards permitted under Prüm).

The pilot involved up to 10,000 exchanges of unsolved UK DNA crime scene profiles with each participating Member State. The reciprocal provision of crime stain profiles to the UK in return was set at a maximum capacity of 3,000 profiles split between the participating Member States. These profiles were searched against an agreed set of profiles containing serious criminals convicted in the UK.

The Metropolitan Police Service (MPS) led the operational delivery of the pilot on behalf of the Home Office. This is because they have the CODIS 7.0 software with a Prüm interface for the matching and reporting of DNA profiles. This links to s-TESTA, an approved secure exchange network between Member States, which was temporarily accredited to go live in the MPS for the duration of the pilot.

Each participating Member State signed a Memorandum of Understanding (MoU) or agreed letters which determine exactly what each country is committing to provide and how the data would be handled. These stipulated the data protection requirements expected from the participants. They were also specific about the handling of the profiles provided and the rules around the retention of any profile by the receiving Member State. In addition an evaluation visit was carried out by the Prüm DNA lead in The Netherlands which involved a data protection sign off on the readiness of the pilot on behalf of the EU Commission.

The Connections

The connection to each pilot Member State was staggered and extensive testing was carried out with test sets before any exchange of live data took place. Each connection had to be phased in agreement with each country and scheduled to fit with their business as usual and system restrictions. The initial exchanges took place with each country over the following period:

17 March 2015 The Netherlands
11 May 2015 Spain
6 August 2015 France
21 August 2015 Germany

Additional exchanges took place with each country within the lifetime of the pilot up to maximum profile exchanges agreed.

The Dataset

Following a stringent verification and risk assessment process, police forces in the UK identified 2,513[54] crime scene profiles from unsolved crimes in their areas to be exchanged with the four Member State pilot countries. All of the crime scene profiles selected were of high probative value, for example blood, semen or saliva left on an intimate area on a victim, and were deemed to have originated from a single source of DNA, as opposed to being from a crime scene profile containing DNA from more than one person. Furthermore, only profiles with a sufficient number of loci would be searched (at least SGMPlus®[55]).

The MPS have also carefully identified approximately 40,000 subject profiles from convicted offenders, drawn from those on the National DNA Database who were convicted or arrested in the Metropolitan Police District. Stringent privacy safeguards are in place, profiles were validated and anonymised and only relate to subjects on the Violent and Sex offender (VISOR) register and those indefinitely retained under PoFA 2012. These formed the subset of the NDNAD that was used to search incoming profiles against. An incoming 750 crime scene profiles was received from each of the 4 participating countries (meeting, in total, the agreed 3,000 profile allocation) to search against all the profiles held on the CODIS database.

The UK crime scene profiles were searched against all profiles on the other Member States' Prüm database whereas the profiles sent to us were only searched against the CODIS database held in the MPS.

Match Types

A forensic DNA profile retained on a DNA Database is a string of numbers. Each value represents a component (allele) at that region of DNA with 2 components (locus-plural loci) for each region, one inherited from each parent. The target regions are areas of DNA known to vary between individuals providing discrimination between people. The larger the number of target regions, the better the discrimination power between different people. None of the DNA regions code for any physical characteristics of a person. Occasionally, a 'wildcard' value is present in a DNA profile string. This represents an unconfirmed value from a rare event or an unknown designation for that DNA profile.

The Prüm Decisions require at least 6 regions of DNA (12 components) must be directly comparable for a Hit notification to be generated. An additional safeguard introduced within this pilot, is only matches containing 10 regions (20 components) or above will be progressed further in the investigation.

For a hit notification to be produced between 2 DNA profiles, four categories of matches have been defined in the Prüm Decisions:

[54] 2,513 were exchanges with France and Germany; 2,500 with The Netherlands; and 2,405 with Spain taking the total outgoing pilot exchanges to 9,931, within the 10,000 permitted.
[55] SGMPlus® which looks at ten loci.

Quality 1. (Q1): This is an **exact match** category. Each DNA value at all components compared match exactly
Quality 2. (Q2): This is an **exact match** category where one or both profiles in a match contain a wildcard at a point of comparison. Additional reviews of the DNA profile(s) at the wildcard can confirm or eliminate a hit.
Quality 3 (Q3): This is a **close match** category with one difference between 2 profiles. The type of difference between the two profiles (known scientifically as a micro variant) is fully defined and understood. Additional reviews of the DNA profile(s) can confirm or eliminate a hit.
Quality 4 (Q4): This is a **close match** category with one difference between 2 profiles. The cause of this may be a typographical error, or be due to a genuine non-match. Additional reviews of the DNA profile can confirm or eliminate a hit.

During the pilot ALL matches (including Q1) carried the safeguard of independent scientific verification of each hit. This involved reviewing the scientific profile image (from which the DNA profile 'string-of-numbers' is derived). As indicated at Table 6, only Q1 and Q4 match categories were identified. Where necessary, the verification process was extended to include the re-profiling of the sample using different DNA profiling kits. This increased the number of DNA components in common in both DNA profiles or was necessary for confirmation of a variant. The purpose was to confirm or eliminate a match before the exchange of personal data.

Results

Table 6 Prüm Pilot Results Table

Profile number	Offence	Submitting force	Country hit is from	Hit Status	MS Profile type	Hit Quality	Operational Status
1	Rape	Police Scotland	France	Verification pending	Stain	4	Awaiting verification. No details on French crime scene sought yet
2	Indecent Assault	Police Scotland	France	Verification pending	Stain	1	Awaiting verification. No details on French crime scene sought yet
3	Rape	PSNI	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
		PSNI	Germany	Verification pending	Stain	4	Awaiting verification, no demographic information exchanged
4	Murder	West Midlands	Netherlands	Verified hit	Person	1	Following enquires with the Dutch authorities hit has been eliminated from the enquiry
5	Murder	West Midlands	Netherlands	Verified hit	Person	1	Following enquires with the Dutch authorities hit has been eliminated from the enquiry
6	Burglary in a Dwelling	MPS	France	Verification pending	Stain	4	Awaiting verification. No details on French crime scene sought yet
7	Burglary in a Dwelling	MPS	Netherlands	No Hit	Stain	4	Following further work this hit was not pursued
8	Arson	MPS	France	Verified hit	Person	1	Hit verified. Demographic details provided. Person eliminated from enquiry due to legitimate access
9	Rape	MPS	France	Verified hit	Stain	1	Hit not pursued as stain-to-person hit more valuable
			France	Verified hit	Person	1	Demographic data provided. Suspect in French prison having been extradited from the Netherlands for similar offences. Suspect believed to be Cameroonian. Investigation ongoing.
10	Burglary in a Dwelling	MPS	Netherlands	Verified hit	Stain	1	Request for demographic details sent to Interpol The Hague 17/08/2015
11	Burglary in a Dwelling	MPS	France	Verification pending	Person	4	Awaiting verification, no demographic information exchanged

12	Burglary in a Dwelling	MPS	Spain	Verification pending	Stain	1	Awaiting verification. No details on Spanish crime scene sought yet. Also French scene-to-scene match and German stain-to-person match
			Spain	Verification pending	Stain	1	Awaiting verification. No details on Spanish crime scene sought yet. Also French scene-to-scene match and German stain-to-person match
			France	Verification pending	Stain	1	Awaiting verification. No details on French crime scene sought yet. Also Spanish scene-to-scene match and German stain-to-person match
			France	Verification pending	Stain	1	Awaiting verification. No details on French crime scene sought yet. Also Spanish scene-to-scene match and German stain-to-person match
			France	Verification pending	Stain	1	Awaiting verification. No details on French crime scene sought yet. Also Spanish scene-to-scene match and German stain-to-person match
			Germany	Verification pending	Person	1	Awaiting verification. Also stain-to-stain match with France and Spain
13	Burglary in a Dwelling	MPS	France	Verification pending	Stain	4	Awaiting verification. No details on French crime scene sought yet
14	Burglary in a Dwelling	MPS	Netherlands	Verified hit	Person	1	Demographic Information provided. Person believed to be Albanian. Circulated domestically; also being sought abroad.
15	Burglary in a Dwelling	MPS	France	Verification pending	Person	4	Awaiting verification. No details on FR crime scene sought yet
16	Burglary in a Dwelling	MPS	Spain	No Hit	Stain	4	Following further work this hit was not pursued
17	Burglary in a Dwelling	MPS	Spain	Verified hit	Person	1	Also stain-person hit in France and stain-to-stain in Germany. Demographic information provided. Person Romanian and known to have been deported previously from France. Police applying to CPS for EAW.
			France	Verified hit	Stain	1	Also stain-person hit in Spain and stain-to-stain in Germany. Demographic data provided following stain to person hits.
			France	Verified hit	Stain	1	Also stain-person hit in Spain and stain-to-stain in Germany. Demographic data provided following stain to person hits.

			France	Verified hit	Stain	1	Also stain-person hit in Spain and stain-to-stain in Germany. Demographic data provided following stain to person hits.
			France	Verified hit	Person	1	Demographic information provided. Person Romanian. Police applying to CPS for EAW. Article 34 (locate/trace) Marker on SISII.
			Germany	Verified hit	Stain	1	Also stain-to-person hit in Spain and France and stain-to-stain in France. Demographic data provided following stain to person hits.
18	Burglary in a Dwelling	MPS	Spain	Verified hit	Person	1	Profile taken in Spain when person was a minor. Letter of Request needed to follow-up case. Police decided not to pursue.
19	Burglary in a Dwelling	MPS	France	Verified hit	Person	1	Demographic data provided. Person Romanian. Police have decided not to pursue case. No property stolen.
20	Burglary in a Dwelling	MPS	France	Verified hit	Stain	1	Also stain-person hit in France and stain-to-stain in France and Germany
			Spain	Verified hit	Stain	1	Also stain-person hit in France and stain-to-stain in France and Germany
			France	Verified hit	Person	1	Demographic details provided person believed to be French. Also stain-to stain in France, Germany and Spain. Person known from a total of 9 countries. Circulated as wanted in the UK.
			France	Verified hit	Stain	1	Request for demographic details sent to Interpol Paris 17/08/2015. Also stain-to-person in France and stain-to-stain in Germany and Spain
			France	Verified hit	Stain	1	Request for demographic details sent to Interpol Paris 17/08/2015. Also stain-to-person in France and stain-to-stain in Germany and Spain
			France	Verified hit	Stain	1	Request for demographic details sent to Interpol Paris 17/08/2015. Also stain-to-person in France and stain-to-stain in Germany and Spain
			Germany	Verified hit	Stain	1	Awaiting verification. No details on German crime scene sought yet. Also stain-to stain in Spain and France and stain-to-person in France.
21	Burglary in Other Buildings	MPS	France	Verified hit	Person	1	Demographic information provided. Suspect believed to be abroad. Will be circulated as wanted domestically. Low value theft, so EAW not being pursued.

22	Rape	MPS	France	Verification pending	Person	4	Awaiting verification, no demographic information exchanged.
			France	Verification pending	Stain	4	Awaiting verification. No details on French crime scene sought yet.
23	Burglary in Other Buildings	MPS	France	Verification pending	Stain	4	Awaiting verification. No details on French crime scene sought yet.
24	Burglary in a Dwelling	MPS	Spain	Verification pending	Stain	1	Also stain-to-stain hit in Spain and stain-person hit in Germany
			France	Verification pending	Stain	1	Also stain-to-stain hit in France and stain-person hit in Germany
			Germany	Verification pending	Person	1	Also stain-to-stain hit in Spain and France
25	Burglary in a Dwelling	MPS	France	Verification pending	Stain	1	Also stain-to-stain hit in Spain and stain-person hit in Germany.
			Spain	Verification pending	Stain	1	Also stain-to-stain hit in France and stain-person hit in Germany
			Germany	Verification pending	Person	1	Also stain-to-stain hit in France and Spain
26	Other Burglary	MPS	Spain	Verified hit	Person	1	Profile taken in Spain when person was a minor. Letter of Request needed to follow-up case. UK DNA hit now being pursued.
27	Other Burglary	MPS	France	Verified hit	Person	1	Person profile held twice on French database under different names. Both are of Romanians. Both names circulated as wanted domestically.
		MPS	France	Verified hit	Person	1	Person profile held twice on French database under different names. Both are of Romanians. Both names circulated as wanted domestically.
		MPS	France	Verified hit	Stain	1	No details on French crime scene stain sought yet. Also hit stain-to-person in France.
28	Rape	MPS	France	Verified hit	Person	1	Person profile held twice on French database, under same name. Person Romanian. Suspect arrested 10 November 2015, in London
			France	Verification pending	Stain	1	Awaiting verification. No details on French crime scene stain sought yet. Also hit stain-to-person in France.

			France	Verification pending	Stain	1	Awaiting verification. No details on French crime scene stain sought yet. Also hit stain-to-person in France.
			France	Verification pending	Stain	1	Awaiting verification. No details on French crime scene stain sought yet. Also hit stain-to-person in France.
			France	Verification pending	Stain	1	Awaiting verification. No details on French crime scene stain sought yet. Also hit stain-to-person in France.
			France	Verification pending	Stain	1	Awaiting verification. No details on French crime scene stain sought yet. Also hit stain-to-person in France.
			France	Verified hit	Person	1	Person profile held twice on French database
29	Burglary in a Dwelling	MPS	Spain	Verified hit	Person	1	Demographic data provided. Person Romanian. Person circulated as wanted domestically.
30	Other Burglary	MPS	France	Verified hit	Person	1	Hit verified. Demographics provided; person believed to be French and in France
			France	Verified hit	Person	1	Person profile held twice on French database
31	Affray	MPS	France	Verification pending	Stain	1	One of five stain-to-stain hits
			France	Verification pending	Stain	1	One of five stain-to-stain hits
			France	Verification pending	Stain	1	One of five stain-to-stain hits
			France	Verification pending	Stain	1	One of five stain-to-stain hits
			France	Verification pending	Stain	1	One of five stain-to-stain hits
32	Other sexual	West Yorks	France	Verification pending	Stain	4	Stain-to-Stain hit.
33	Other sexual	MPS	France	Verification pending	Stain	4	Stain-to-Stain hit.
32	Rape	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
33	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	1	Awaiting verification, no demographic information exchanged
34	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	1	Awaiting verification, no demographic information exchanged

35	Other Sexual	Kent Police	Germany	Verification pending	Person	1	Awaiting verification, no demographic information exchanged
36	Attempted Rape	Essex Police	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
37	Rape	Lincolnshire Police	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
38	Rape	West Mercia	Germany	Verified hit	Person	1	Person identified. Circulated on Article 34 of SISII (locate/trace).
39	Other Sexual	Greater Manchester Police	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
40	Rape	Greater Manchester Police	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
41	Rape	Leicestershire Police	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
	Rape	Leicestershire Police	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
42	Indecent Exposure	Lancashire	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
43	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
44	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
45	Burglary in Other Buildings	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
36	Burglary in Other Buildings	MPS	Germany	Verified hit	Person	1	Demographic information provided. Circulated as wanted on domestic system. Person Hungarian.
47	Burglary in Other Buildings	MPS	Germany	Verified hit	Person	1	Person identified. Romanian. Circulated domestically and on SISII (locate trace). Burglary value too low for EAW.

48	Burglary in Other Buildings	MPS	Germany	Verified hit	Person	1	High Value burglary. Demographic information provided. Person Romanian. Circulated as wanted domestically.
49	Burglary in Other Buildings	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
50	Burglary in Other Buildings	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
51	Business Property	MPS	Germany	Verification pending	Person	1	Awaiting verification, no demographic information exchanged
52	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
53	Burglary in a Dwelling	MPS	Germany	Verification pending	Stain	4	Awaiting verification, no demographic information exchanged
54	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
55	Burglary in Other Buildings	MPS	Germany	Verified hit	Person	1	Demographic information sought from Germany
56	Burglary in Other Buildings	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
	Burglary in Other Buildings	MPS	Germany	Verification pending	Stain	4	Awaiting verification. No details on German crime scene sought yet
57	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
58	Other Burglary	MPS	Germany	Verification pending	Stain	4	Awaiting verification. No details on German crime scene sought yet
59	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	1	Awaiting verification, no demographic information exchanged

60	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
61	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
62	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
63	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	1	Awaiting verification, no demographic information exchanged
64	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	1	Awaiting verification, no demographic information exchanged
65	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
66	Burglary in a Dwelling	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
67	Other Sexual	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
68	Other Sexual	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
69	Other Sexual	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
70	Rape	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
71	Rape	MPS	Germany	Verification pending	Stain	4	Awaiting verification. No details on German crime scene sought yet
72	Rape	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
73	Other Sexual	MPS	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
74	Rape	MPS	Germany	Verified hit	Person	1	Demographic details provided. Person Romanian. Circulated on domestic systems. Police working with Romanian authorities to trace individual. Police considering with CPS whether to issue EAW.
75	Other Sexual	West Midlands	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged

76	Rape	Police Scotland (Strathclyde)	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged
77	Rape	Police Scotland (Strathclyde)	Germany	Verification pending	Person	4	Awaiting verification, no demographic information exchanged

Case Study:
A DNA crime scene profile from an attempted rape, recovered from blood after the victim had managed to smash a glass on her attacker's head, was sent to all four Prüm pilot countries. The profile, hit against a person/subject profile held in France following an arrest there for a burglary. Following the verification of the hit, and after further co-operation with France via the National Crime Agency, demographic information was sought and provided on a Romanian national. This individual was stopped in London on 10 November 2015 on suspicion of a motoring offence which would not have led to a DNA swab being taken or searched domestically. However due to the Prüm hit, when he supplied his demographic details the warrant for his arrest was revealed and he was arrested and charged with the attempted rape. He is currently on remand.

The validity of all of the UK crime scene profile hits against other Member State Prüm DNA Database records was assessed by MPS Forensic Scientists to ensure there was a scientific assessment of the result before they were forwarded to the NCA UKICB for Interpol to request demographic data.

For the purposes of the pilot and as an additional safeguard, had there been any, the MPS would have scientifically verified any hits that the other Member States received from their searches against our CODIS database, which is not normal practice within a full Prüm operational environment. In addition, a questionnaire was designed to follow up the data handling of any such hits in the Member States.

The databases of the four Prüm member states (Netherlands, Spain, France and Germany) participating in the UK Prüm pilot contain 79% of the approximately 5 million total person profiles potentially available through the Prüm database, and 73% of the approximately 0.7 million total crime scene stains[56].

Matching the 2,513[57] UK pilot crime scene profiles against the databases of the four member states above yielded 71 scene-to-person matches (2.8% of the 2,513 sample) and 47 scene-to-scene[58] matches (1.9% of the 2,513 sample).

As at 31 March 2014, the UK National DNA database (NDNAD) contained approximately 170 thousand unmatched crime scene profiles. In each year (April 2010 to March 2014) an average of 36 thousand new crime scene profiles have been uploaded to the NDNAD with an average 61% chance of being matched to a person profile when searched against the NDNAD.[59] On this basis, potentially, each year there could be around 14 thousand new unmatched UK crime scene profiles.

Because of the way the UK pilot sample was selected, the similarity of match rates for all crime scenes cannot be checked from the results. This means that scaling up from the pilot results to predict the results of searching all 170 thousand unmatched crime scene profiles held on the NDNAD against the Prüm database can only be regarded as speculative.

Although the UK Prüm DNA exchange pilot only yielded a relatively small number of hits, it suggests that UK participation in Prüm could generate new evidence to support conclusion of some serious crimes, both from scene-to-person and scene-to-scene DNA matches. Furthermore, EU-wide Prüm participation also offers an

---

[56] Source: Note from the General Secretariat of the Council of the European Union to the Working Party on Information Exchange & Data Protection regarding 'Prüm Decisions' : statistics and reports on automated data exchange for 2014. Total number of person profiles on Dutch, Spanish, French and German databases 4,073,004; and total number on the entire Prüm DNA database 5,174,903. Total number of crime scene stains on Dutch, Spanish, French and German databases 524,563; and total number on the entire Prüm DNA database 721,020. Figures as at 31/12/2014. http://data.consilium.europa.eu/doc/document/ST-5503-2015-REV-2/en/pdf

[57] The total number of UK person profiles submitted for matching was 2,513; of these, all were submitted for matching against the French and German databases, 2,500 for matching against the French database and 2,405 for matching against the Spanish database.

[58] A scene to scene match is one where the same DNA profile was generated from crime scene stains at different crime scenes but no match has been made to an individual.

[59] Source: National DNA Strategy Board, Annual Report 2013-2014. As at 31/03/2014 there were 168,519 unmatched crime scene profiles on the NDNAD. Approximate number of new crime scene profiles added (in thousands): 40 in 2010-2011; 39 in 2011-2012; 33 in 2012-2013; and 35 in 2013-2014. Chance of matching a new crime scene profile to a person profile when searching against the NDNAD: 52.9% in 2010-2011; 61.1% in 2011-2012; 61.4% in 2012-2013; and 61.9% in 2013-2014. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/387581/NationalDNAdatabase201314.pdf

opportunity to build knowledge about cross-border criminal activity. The scene-to - person and scene- to- scene hits in the pilot included the following:

- Verified scene to person hits for rape, murder and arson where demographics have been requested and/or received via Interpol and the NCA and investigations are ongoing.

- One UK crime scene profile linked to burglary matched to a Netherlands crime scene profile which The Netherlands had separately matched to a person profile on the Polish Prüm database and leading to a UK Interpol request to Poland.

- One UK crime scene profile from a burglary in a dwelling matched to a French database crime scene profile, a Spanish database crime scene profile and a German database person profile. This is suggestive at this stage of a pattern of cross border offending.

- One UK crime scene profile from a burglary in a dwelling matched to two Spanish database crime scene profiles, a German database crime scene profile, three French database crime scene profiles and a French database person profile.

Benefits

The key UK strategic benefits envisaged from the Prüm Decisions are:

Simplified processes to request information and/or data: Many of the current EU-wide intelligence gathering processes are not readily understood and, in some instances are cumbersome and cannot be executed in a timely manner. Prüm would simplify the process, encouraging greater sharing of information as a routine activity. An automated step that produces a hit provides the reason for the request for the follow up information and increases the likelihood that the request will be accepted. This could assist in the identification of potential serious offenders and in providing valuable intelligence in relation to counter terrorism investigations.

Efficiency gains in international searching: Allowing many more enquiries to be processed, including simultaneous searches against other Member States' databases, without the need for additional work would mean that UK law enforcement agencies can establish whether an individual is known in another Member State or eliminate a line of enquiry much earlier in the investigation. In turn, this means more targeted police to police or Mutual Legal Assistance requests (incoming and outgoing).

Increase in resolution of unsolved crimes: The capability to search more databases simultaneously will enable the UK to review criminal cases that are currently unsolved. This could lead to earlier detention, and subsequent conviction of individuals. Whilst this is possible now, the increase in flow of information and data should also cause an increase in the potential for a match with unsolved crime data.

Improved response to requests for information associated with crime and terrorism: The increase in speed of response offered by Prüm would decrease the

time required to identify potential offenders and people involved in crime and terrorism. This more rapid identification of people of interest could lead to early detention or operations to prevent loss of life and/or property**.**

Case Study 1: Austria May/June 2015
21 May 2015 double homicide and robbery case in Vienna with an elderly couple executed. One body was unclothed and inscribed with words in Latin. Valuable items not stolen but less valuable ones are. The offender remained for several hours beside the dead bodies. Austrian profilers assume crime committed by a potential serial killer.
29 May 2015 noon: DNA profiles from the offender which loaded in national DNA Database with No Hit result. Fully automated Prüm searches start minutes after this national search. Hit to a reference profile, stored in The Netherlands (NL) and additionally to an open stain stored in Germany (DE). Forensic confirmation carried out immediately and on afternoon of same day the second step follow up request background information made to NL and DE.
2 June 2015 responses received from both countries. The NL reference profile sprang from a Polish offender. He was sampled and stored in the NL after committing grievous bodily harm in 2011. The DE open stain profile was secured in DE in January 2015 after a burglary case in a grocery.
With fingerprints, Austria then obtained further Prüm AFIS person hits in NL, Poland and DE. The whereabouts of the offender was not known in all concerned states.
3 June 2015 a worldwide arrest request issued.
8 June 2015 offender located and arrested in Düsseldorf, Germany.

Exploitation of UK investment in other data systems: The UK has already invested in technical solutions and processes to support exchange of international data. These are successful, but Prüm would create a “front end” to these that establishes, simply and quickly, whether a Member State holds relevant data, information or intelligence. This would increase the volume of information shared and result in greater, more-effective and efficient use of current data system exchange processes and technology.

Case Study 2: Finland
Following a series of burglaries in Finland, DNA recovered from a crime scene was sent via Prüm and matched a profile held in the Lithuanian DNA database. Following the provision of demographic data the Finnish Police were able to track the criminal’s movements to and from Finland using passenger records from ships he had used. He could also be linked to other individuals who had travelled with him. This enabled a gang of travelling burglars to be identified. The original perpetrator was arrested and later found guilty of 64 burglaries and sentenced to four years in prison. Fingerprint matching proved he was known in Austria; there was also a DNA match to crime scene profiles from Sweden. Exchanges through Interpol additionally revealed he was wanted by the Norwegian authorities.

Detection of volume crime as well as serious crimes: There is currently no other mechanism for detecting volume crime. Prüm would therefore meet a currently suppressed demand which may lead to improved public confidence in policing.

Enhanced crime and terrorism intelligence picture: Evidence from countries already operating Prüm has indicated that Prüm has the potential to identify patterns or associations that would otherwise not be apparent. In Counter Terrorism the Prüm arrangements have the potential to enhance and add significantly to the protection capability that is already in place. There are well developed fingerprint databases in the EU with the potential to search a dataset in excess of 26 million, this would greatly assist the fight against terrorism and protect the UK.

Access to Eurodac for criminal investigation searching: Eurodac is the EU-wide database of asylum-seekers' and illegal migrants' fingerprints, which currently stands at approx 2.9m prints, which was set up to assist in determining which Member State is to be responsible pursuant to Regulation (EU) No 604/2013 [the 'Dublin III' Regulation] for examining an application for international protection lodged in a Member State by a third-country national or a stateless person. Law enforcement agencies across Member States have recently[60] been granted access to this database for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences. However, one of the conditions that must be satisfied before such access is granted is that a Prüm search must have already taken place. This currently bars the UK from accessing this database for law enforcement. Joining Prüm would lift this restriction.

Operational policing in the UK recognise the potential benefits that automated access to a wider pool of DNA, fingerprint and vehicle registration databases across Europe for the prevention and detection of crime bring.

Risk

It is important to strike an appropriate balance between the public interest in the prevention and detection of crime and the individual's right to privacy, particularly in circumstances where that individual has never been convicted of an offence.

The key objections to the UK joining Prüm, as voiced by public interest groups and others[61] consulted by the Home Office have been the potential for UK citizens who had never been convicted to be identified as suspects of crime in another Member State following a DNA/fingerprint match or (in the case of DNA) that the match is not a true one. These matters are covered in detail in the annexes and set out further below.

Conviction Only DNA Profile and Fingerprint Searching
In accordance with stated policy, if Parliament votes to rejoin the Prüm Decisions, it is the intention of the Government to allow Member States to only search the DNA profiles or fingerprints of those who have been convicted in the UK.

DNA Adventitious Matches:
Chapter 1 of the Annex of Prüm Decision 2008/616/JHA states:

[60] Accessing this database for law enforcement purposes went live on 20 July 2015.
[61] Justice, Fair Trials International, Big Brother Watch, Gene Watch UK, DNA Ethics Group, Liberty, the Biometric Commissioner, Information Commissioner's Office

The DNA-profiles made available by the Member States for searching and comparison as well as the DNA-profiles sent out for searching and comparison must contain at least six full designated (1) loci and may contain additional loci or blanks depending on their availability. The reference DNA profiles must contain at least six of the seven ESS [European Standard Set] of loci. In order to raise the accuracy of matches, all available alleles shall be stored in the indexed DNA profile database and be used for searching and comparison. Each Member State should implement as soon as practically possible any new ESS of loci adopted by the EU.

It is widely accepted that DNA profile matches of 6 and 7 loci have a high probability of being adventitious (DNA profiles from two individuals, who are not identical twins, which match by chance).

A statistical analysis [Annex H] by Principal Forensic Services Ltd. (PFS) was commissioned in order to examine the likely impact of Prüm exchange on the UK and to make recommendations to assist in the development of robust business processes to mitigate risks.

DNA database data was provided from 14 Member States (including the UK) which informed the study. The analysis was completed in September 2014. Key recommendations and findings from the PFS study included:

- More adventitious matches occur with 6 loci (approx. 26-38% true matches) and 7 loci (approx. 82-94% true matches). With 8 loci and above, c.98% or more of the matches observed will be true matches

Therefore the Government has decided that, should Parliament vote to rejoin Prüm, the UK would adopt higher standards on DNA loci than the minimum stipulated in the Prüm decisions and would accept the recommendation of the PFS study that:

- Only crime scene profiles with more than 8 loci should be shared with other Member States on the UK Prüm exchange. This is to ensure that the level of adventitious hits is kept within acceptable and manageable levels.
- The UK should share its subject profiles with other Member States but demographic data for subjects should only be 'routinely' shared following the match of 10 or more loci. (Note this does not rule out further work on 'weaker' hits in order to try and increase the number of matching loci or the sharing of specific intelligence, particularly for more serious crimes which are under investigation. Verification by forensic scientists on a case by case basis further mitigates any action on adventitious matches).

In addition many Member States' DNA profiles are now stored using the new European Standard Set (ESS) of loci. For those countries which retain large numbers of 10 loci profiles, all are using chemistry (SGMPlus®) which is compatible with that used by the UK for the majority of its profiles. As a result, with diminishing percentages of profiles with fewer than 10 loci held, the risk of false positives also diminishes. The only exception is Germany, which still has a large number of 7 and 8 loci hits, which could produce adventitious matches, albeit on an ever decreasing scale as they now also use the ESS. In these instances other DNA tests might be

applied to increase the number of comparable loci and eliminate adventitious matches (see sub section on Match Types in the Pilot section).

Table 7 Loci Make up of Profiles held on DNA Databases from the PFS Study

Country	% profiles with 12 or more loci	% profiles with exactly 10 loci	Number of profiles	Notes
Spain	99.92% persons 93.56% stains	N/A	65,437 Crime scene 260,010 person	
Austria	31.20%	46.88%	25,320 Crime scene 179,772 person	10 loci SGM+
Cyprus	90.71%	N/A	10,765	
Czech Republic	96.08%	N/A	138,832	
Estonia	23.50%	76.49%	27,800	10 Loci SGM+
Finland	17.96%	79.66%	162,857	10 Loci SGM+
France	92.24%	N/A	2,723,867	
Germany	32.4%	N/A	1,037,006	24.15% 7 loci 29.14% 8 loci
Hungary	96.02%		37,734	
Lithuania	34.15%	64.29%	70,621	10 Loci SGM+
The Netherlands	41.78%	54.77%	230,016	10 Loci SGM+
Poland	22.19%	76.48%	38,681	10 Loci SGM+
Romania	95.77%	N/A	22,419	
Slovenia	N/A	100%	33,890	10 Loci SGM+

Automated release of VRD

Unlike DNA and Fingerprints, Prüm VRD searches lead to automated release of VRD including personal information. The safeguarding section below sets out the strict data protection rules that apply to ensure that the data is only used for the purpose it is requested and the audit processes applied to ensure that anyone who accesses the data is identifiable. In addition the data is identical to that which will already be available under the Cross Border Enforcement Directive set out in Option 1. Access to VRD under the Cross Border Enforcement Directive will incorporate the vast majority of requests.

Jurisdiction of the Court of Justice of the European Union (CJEU)

The current Government would not have ceded CJEU jurisdiction over the field of policing and criminal justice during negotiation of the Lisbon Treaty.

It is clear that accepting CJEU jurisdiction over measures in the field of policing and criminal justice is not risk free. This is because the CJEU can rule in unexpected and unhelpful ways. The Metock judgment in the field of free movement is a prime example of this. It is more difficult to reverse the effects of a judgment by the CJEU than it is to reverse the effects of a judgment by the UK Supreme Court, which can be done through domestic legislation. At the EU level changes would generally

require the support of a qualified majority of Member States and the European Parliament, which is more difficult to obtain.

The Government considers, however, the risk of CJEU jurisdiction to be at its greatest as concerns matters relating to substantive criminal law. This is a matter that should be determined by our sovereign Parliament, particularly given that the relevant measures are often open to wide interpretation. This also reduces the risk of the EU obtaining exclusive external competence in relation to such matters. Equally, the Government would generally be concerned about the EU entering into third country agreements with other States as this is something that should largely be done by the Government in this sensitive area in order to ensure our interests are best served. Where a measure deals with cooperation with other Member States the Government will balance the risk of CJEU jurisdiction against the potential benefits the new measure can bring.

Volume of Work
The UK's criminal fingerprint and DNA databases are significantly larger than those in other Member States. There is a risk that there will be a high volume of follow-up work (for example interviewing those revealed by DNA or fingerprint hits to have been present at the scene of a crime) for the police, Crown Prosecution Service, Crown Office, Public Prosecution Service for Northern Ireland, Courts and the NCA. In mitigation of this:

- The evidence from other Member States suggests that they have not been overwhelmed with follow up work, despite being connected to multiple other Member States.
- Connections to Member States via Prüm are an iterative staged process with connections for DNA, fingerprints being made one Member State at a time. Therefore it is possible to control the speed at which connections and therefore information flows take place.
- Fingerprint exchange is additionally managed by quota levels and the flow of outbound requests is controlled by the Member State so that volume of search requests will not exceed capacity to respond to matches.
- DNA Bulk Comparison exercise would also be part of a staged approach, minimising significantly the volume of work at any one time. The PFS study concluded that the anticipated initial match rate as a result of the bulk exchange with all other Member States is estimated to be 14,000 true matches.
- The potential inbound volumes as a result of Prüm are not known at this time but it is fair to assume that the relative ease of access via Prüm could increase the overall volume of inbound requests compared to the number of inbound Interpol requests that are currently made. However, these would be filtered through the automated matching systems negating the manual process currently required at this stage.
- Follow up requests may also increase, however the resulting police to police or Mutual Legal Assistance requests will be much more targeted as it will already have been ascertained that there has been a match within the UK databases.

Cost
The infrastructure and running costs to the UK of rejoining Prüm are set out in the implementation section and have a rough order of magnitude of £13.5Mn. However,

these costs are significantly reduced from the costs of £31Mn (£49Mn in today's money[62]) that the, then, Government in 2008 was willing to accept at a time when the national database infrastructure was fragmented.

Member States and Prüm

The Home Office, in partnership with Sustainable Criminal Justice Solutions, secured European Commission funding from the Prevention of and Fight against Crime Programme to conduct the UK Prüm Fingerprint Evaluation Project and the UK Prüm DNA Evaluation Project. Both projects were designed to explore the experience of Member States that are currently operational under Prüm to understand any potential impact, benefits, risks, costs and solutions for the UK in participating in the Prüm Decisions. In addition, the Home Office conducted a survey of Member States experience of VRD exchange under Prüm.

UK Prüm Fingerprint Evaluation Project (UKPFE)

This report[63] concentrates on the dactyloscopic (fingerprint) element of the Prüm Decisions which enable a Member State to search the fingerprint databases of other Member States on a hit / no-hit basis where a response advises whether a match has been found in the database(s) searched.

Table 8 Prüm Statistics: automated fingerprint data exchange 2014[64]

	TP/TP		LT/UL - - LP/ULP		LP/PP - - LT/TP		TP/UL - - PP/ULP	
	sent	verified hits	sent	verified hits	sent	verified hits	sent	verified hits
Bulgaria	22	0	1	0	40	0	23	0
Czech Republic	144	30	154	141	267	247	187	150
Germany	24,862	1,203	314	14	31,450	276	1,215	11
Spain	2,725	182	83	1	4,607	40	406	2
France	3,096	333	2,573	0	8,017	47	2,087	3
Cyprus	508	3	145	0	1,930	1	770	0
Lithuania	10	0	14	0	2	0	10	0
Luxembourg	377	20	8	0	1,275	6	12	0
Hungary	73	0	78	0	81	0	22	0
Malta	0	0	0	0	16,668	0	0	0
The Netherlands	7,638	240	0	0	2,843	14	4,775	0
Austria	57,781	3,186	7	0	5,337	49	498	0
Romania	760	59	684	0	888	42	1,274	0
Slovenia	2,766	48	0	0	3,628	3	2,277	3

[62] After taking account of inflation £31Mn would be worth about £38.5Mn with the equivalent value as around £49m today (38.5Mn X 1.035^7).

[63] To be published shortly

[64] Source data: http://data.consilium.europa.eu/doc/document/ST-5503-2015-REV-2/en/pdf

Slovakia	46	8	122	2	503	18	9	3
Finland	24	1	1	0	434	6	0	0
	100832	5313	4184	158	77970	749	13565	172
%		0.0526916		0.0377629		0.0096063		0.0126797

TP/TP: ten-print against ten-print
LT/UL--LP/ULP: fingerprint latent against unsolved fingerprint latent – palm print latent against unsolved palm print latent
LP/PP--LT/TP: palm print latent against palm print--: fingerprint latent against ten-print
TP/UL-- PP/ULP: ten-print against unsolved fingerprint-- latent palm print against unsolved palm print latent

Findings of UKPFE

Strengths

The Member States taking part in the study recognised the crime solving potential of Prüm as an additional investigative tool for operational police officers:

- Searching latents with all other Member State fingerprints, unsolved crimes can be solved by identifying a person to which it relates in another Member State database.
- Opportunity to link latents and their "owner" to other unsolved crimes.
- Chain of events that follows a hit can lead to multiple arrests and assist in establishing the true identity and whereabouts of offenders across the EU.
- Can help reveal crime trends and patterns.
- System works very quickly, with the result of a search being returned within minutes of it being sent.
- The verification sits with the requesting Member State and therefore it is more cost and time effective for the requested Member State.
- Time and cost effectiveness has been highlighted by a number of Member States, who welcome the need for fewer personnel and resources compared with those required to manage the "classic" fingerprint exchange mechanism through Interpol.

Weaknesses

- Awareness of Prüm - Prüm relies on Member States sending fingerprints for searching against other Member States databases, which will only work effectively if those working in law enforcement are aware of this capability.
- The palm prints comparison system would benefit from further development as it does not currently set out the location within the palm print that a latent palm print has matched, making verification a lengthy process.

Opportunities

- Raising awareness of Member States' national law that impacts on the Prüm process.
- Sharing best practice so that non-operational Member States can benefit from the experience of others.

Threats

- That the gap created by lack of implementation by some Member States allows criminals to continue offending across borders without the ability for law enforcement to make use of fast and efficient fingerprint exchange. When these Member States continue using the "classic" route for fingerprint exchange, the Prüm system is jeopardised as it takes additional resources to facilitate both methods of exchange.
- That the information of innocent people is released following a hit. To mitigate this, Member States apply their own data protection legislation to the information they disclose, which allows the NCP to withhold information should they regard the hit to be against a profile that they do not want to respond to.
- The volume of exchange must be managed carefully, as if the workload increases significantly, and the resources allocated cannot cope with the demand, the system will not work as efficiently as it currently does. Thus it is important that a national search has been conducted and an international element to the crime is considered.

UK Prüm DNA Evaluation Project

This report [65]concentrates on the DNA element of the Prüm Decisions which enable a Member State to search the DNA databases of other Member State on a hit / no-hit basis where a response advises whether a match has been found in the database(s) searched. This does not provide any of the personal details relating to the profile of that hit i.e. the matching of DNA profiles is conducted as a purely numerical process based upon the allele values of the loci being compared. If there is a hit, the searching Member State is responsible for verifying the possible match, and if confirmed, that Member State can then request the follow-up information via the National Contact Point (NCP) in accordance with their national law. In addition, any responses with the personal data to which the DNA profile belongs, is returned in accordance with national law.

At the time of writing this report 21 of the 28 Member States were exchanging DNA profiles with at least one other Member State through Prüm.

[65] To be published shortly

Table 9 Prüm Statistics: automated DNA data exchange 2014[66]-DNA Match statistics counting **own** stains and persons independent of sending direction

Country	Number of DNA crime scene stains as of 31/12/14	Number of DNA person profiles as of 31/12/14	Number Stains own - sent	Hits Stain own - Person ex	Hits Stain own - Stain ex	Hits Person own - Stain ex	Hits Person own - Person ex	total	Total MS with Hits
Belgium	39187	31320	25,913	3255	1654	351	249	5509	2
Bulgaria	1221	15523	2,341	294	69	4	145	512	8
Czech Republic	15081	143350	131,944	360	243	878	1,546	3,027	9
Germany	264847	832695	480,751	3,529	2,998	2,210	8,195	16,932	14
Estonia	10560	46494	1,719	24	6	94	1,931	2,055	9
Spain	64334	286028	60,840	1,231	735	989	2,542	5,497	13
France	154037	2752953	N/A	1,577	1,866	5,630	6,126	15,199	15
Cyprus	13053	976	3,715	8	2	0	0	10	4
Latvia	4493	51366	3,600	38	17	19	58	132	6
Lithuania	4406	76349	13,944	102	38	592	1,212	1,944	14
Luxembourg	3182	2121	2,672	305	195	51	197	748	6
Hungary	5412	120765	30,641	63	41	139	894	1,137	7
Malta	449	30	842	0	0	0	0	0	0
Netherlands	41345	201328	26,000	881	1,227	1,059	1,573	4,740	19
Austria	26375	186924	445,304	1,486	1,327	1,516	5,974	10,303	17
Poland	5958	37467	4,800	77	37	143	322	579	14
Romania	948	25441	26,164	25	111	345	1,148	1,629	12
Slovenia	6865	29332	7,945	77	109	125	354	665	11
Slovak Republic	9620	46821	N/A	231	285	232	1,247	1,995	15
Finland	18057	150188	168,193	203	105	220	2,216	2,749	8
Sweden	29772	143061	67,000	375	49	187	543	1,154	6

In addition to commissioning the PFS statistical study (results set out above), the project focussed specifically on the process, procedure and legislation that would enable the UK to share demographic data following a validated 'hit' and made recommendations.

Table 10 UKPDE Recommendations

No.	Recommendation
1	The UK should not automatically supply follow up data on receipt of a request from another Member State. No other Member State currently supplies follow up information in an automated way. A degree of human intervention is required both nationally and locally to ensure information is not shared that could interfere with

[66] Source data: http://data.consilium.europa.eu/doc/document/ST-5503-2015-REV-2/en/pdf

	ongoing intelligence gathering and/or criminal investigations being conducted by UK Law Enforcement Agencies (LEAs), affect the integrity of witness protection arrangements or to identify issues that may impact upon National Security if the requested information is provided.
2	The following considerations should be incorporated into UK follow up processes: • Law Enforcement Led (Investigators) • Opportunity led i.e. only apply resources where needed with consideration of the seriousness of the offence • A decision by the relevant LEA as to whether or not follow up information is required • Where possible establish 'police to police' communication channels with other Member State rather than using prosecutor channels (as these tend to cause lengthy delays in the exchange of information) • An automated / mandated collation of performance data (quantitative and qualitative) relating to the hit and post hit process
3	If the UK opts to implement Prüm DNA exchange the issues of preferred communication channel and request format should be agreed between the UK and each Member State as part of the phased implementation plan until such time as a universal approach is adopted by all participating Member State.
4	With regards to timescales for response to follow up requests from other Member State it is recommended that Article 4 of Swedish Initiative 2006/960/JHA3 should be applied at least for priority cases)
5	It is recommended that the capture of management information is integral to the UK post hit processes and that if the UK progress to implementation of Prüm suitable automated means of capturing the performance data relating to post hit processes is identified.
6	To reduce the possibility of adventitious matching only crime scene stains with at least 8 loci present should be routinely loaded onto a UK 'Prüm Database'. Provision to allow LEAs to request the loading of profiles with less than 8 (but at least 6 for Prüm compliance) loci present should be made to enable investigators involved in the most serious crime types to conduct an international DNA search.
7	Whilst all UK subject profiles should be made available for other Member States to search against, follow up requests for demographic data should only routinely be allowed where a minimum of 10 loci have been matched and validated. Requests where matches of less than 10 loci will need to be assessed on a case by case basis following application by the Member State through MLA channels. In such cases data should only be released following a documented, risk assessment process.
8	The current 'International DNA Searching Policy for the UK' (latest version dated 20th February 2014) should be revised as part of the implementation process should the UK seek to engage with Prüm. In particular, the function of the NDNAD SB in authorising the release of data must be reconsidered in light of the anticipated increase in requests from international authorities.
9	The National Crime Agency should remain the UK's National Contact Point for the international exchange of DNA related demographic information and data[67].
10	When subject profiles and associated data are shared with international authorities they must be sent with explicit conditions on their use to include non-retention of profiles on international databases.

[67] Excepting ECRIS criminal record exchange via ACRO and counter terrorism via the MPS.

11	The Home Office should ensure that the Business Implementation Case being prepared for consideration by the UK Parliament contains a Privacy Impact Evaluation concerning the exchange of data via Prüm.
12	Regardless of whether or not the UK decides to engage with Prüm the policy on international data sharing for DNA should reflect the ICO's direction i.e. outgoing requests for information to other Member States should be compliant with the Data Protection Act 1998 whilst incoming requests for information from Member States should be considered against the EU Data Protection Directive.
13	The evidential value of a crime scene profile obtained from a foreign crime scene must be established prior to the release of related demographic data from a matching subject profile held on the UK NDNAD. This should include the 'context' of DNA samples recovered from a crime scene and the type of that sample.
14	Where possible communication channels between the EU and other Member States should be on a police to police basis with information exchanged only used for intelligence purposes.
15	The UK considers how best to collect, store and report on the management information generated by the post hit processes.
16	It is recommended that the UK should routinely provide (and request) the following minimum information in response to (or when making) a follow up request on a hit that meets the agreed UK threshold: • Full Name; • Date Of Birth; • Last Known Address; • Place Of Birth (If known); • Photograph; • Fingerprints (Ten Prints); and, • Criminal Convictions

Anecdotal Evidence

The views of other Member States on Prüm as a whole are universally positive. For example Finland have stated that "Prüm data exchange, when properly resourced (quality and quantity) offers an efficient tool to fight cross-border crime" and Germany's view is that "the police, the justice and the politics do believe that Prüm is a great advantage to criminal justice." Member States provided examples of cases where Prüm had led to a successful case conclusion. The Prüm statistical package does not analyse follow-up work. Even if it did, there is no method, other than individual analysis of each case, to discover whether the hit was evidential or provided a useful investigatory lead or not. Therefore the examples provided were anecdotal [Annex I].

Table 11 Member State Anecdotal Case Studies

Country	Crime	DNA or fingerprints	In which country was the match?	Nationality of person hit against	Outcome/result
Netherlands	1994 Murder	DNA	Germany	**German** (Hit was from initial mass comparison exercise)	Case transferred to Germany with person being convicted in 2009.
Germany	Murder	Fingerprints	Bulgaria	**Bulgarian**	Follow up information requested from Bulgaria was submitted within 3 hours and immediately entered into SIS. The individual was arrested in Austria the next day.
Netherlands	Rape (of 19 year old woman)	DNA	France	**Bosnian**	In 2011, the person was arrested in Croatia, extradited to and convicted in the Netherlands.
Netherlands	2012. Shop robbery (by 3 people - one of the employees seriously maltreated)	DNA (of two of robbers)	Lithuania	**Lithuanian**	In 2014, one person was arrested in Lithuania and extradited to the Netherlands. The other was arrested in the UK and also extradited to the Netherlands. Both in jail and waiting for trial.
Cyprus	2012 house burglary	Fingerprints	Slovakia	**Romanian** (print sent to all active Prüm fingerprint members and a hit was obtained	In April 2013, the person was arrested in Cyprus and extradited to Austria.

				with Slovakia on a Romanian citizen who was also wanted in Austria)	
Slovenia	2003 rape (young girl)	DNA	Spain	**Romanian** (Hit was from initial mass comparison exercise)	EAW issued. Within 3 days the person was arrested in Spain and extradited to Slovenia where he is currently serving a 10 year prison sentence.

Vehicle Registration Data

The exchange of VRD under Prüm would support other EU and national initiatives such as SISII and the police national database (PND) and would bring elements of operations, such as Trivium[68] into everyday policing.

It is currently simpler for police to pursue a British registered vehicle than a foreign registered one. Prüm helps level the playing field for national and foreign registered vehicles.

Member States use of Prüm VRD

Table 12 Prüm VRD requests[69]

Request Made Of	Total Requests	Information Provided
Austria	159447	26632
Belgium	529853	300561
Bulgaria	337835	97208
Cyprus	10635	19
Germany	474360	266092
Spain	315860	133349
France	716986	363801
Finland	206718	3675
Luxembourg	293977	79605
Lithuania	269800	56368
Netherlands	414311	178591
Poland	815533	384156

[68] See Option 1
[69] http://data.consilium.europa.eu/doc/document/ST-5503-2015-REV-2/en/pdf

Romania	352617	112523
Sweden	90598	8292
Slovakia	200465	20659
Slovenia	158144	7087
Total	5347139	2038618

Note 1: Prüm VRD requests can be made concerning a number plate or Vehicle Identification Number (VIN). Number Plate requests tend to be made only to the country of registration; replies provide information only in relation to that country. VIN requests can be made to all countries as the VIN number can be used to track a vehicle through all counties of registration. If a vehicle has never been registered in that country, a "no information held" response will be sent.
Note 2. Some countries use the EUCARIS system to make requests of their own licensing authorities, for example for VIN details
Note 3. Each country can also reply with an error message

Anecdotal feedback from Member States suggests that Prüm has been instrumental in tackling vehicle crime such as the selling and re-registration in another MS of a vehicle that has been stolen, scrapped or written off.

The Prüm Council Decisions need to be understood in conjunction with the Cross Border Enforcement Directive (CBE) and the Second Generation Schengen Information System (SISII). These are both EU measures which wholly or partly relate to vehicles. The table below sets out the differences between the three instruments with regard to vehicles.

Table 13 CBE/SISII and Prüm

	CBE Directive	SISII	Prüm
Title	Directive 2015/413 of the European Parliament and of the Council of 11 March 2015 facilitating cross-border exchange of information on road safety related traffic offences	Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)	Council Decision 2008/615/JHA of 23 June on the stepping up of cross-border cooperation, particularly in combating terrorism and cross border- crime
What does the instrument enable?	The exchange of VRD through EUCARIS – the European Car and Driving License Information System. Information is exchanged in real-time or by batch.	Sharing real-time information on objects of interest to law enforcement (e.g. stolen vehicles) via an 'alerts'. The UK went live on 13 April 2015 In the UK SIS II alerts	The exchange of VRD through EUCARIS – the European Car and Driving License Information System. Information is exchanged in real-time and within 10 seconds

		are made available via the Police National Computer (PNC) and equivalent Border Force systems	
Coverage of measure	Road traffic offences of: • speeding • failure to stop at a red light • use of a forbidden lane • drink driving • drug driving • failure to wear a seat belt • failure to wear a safety helmet • use of a mobile phone or other communications device when driving	Alerts relating to people or vehicles requiring specific checks or discreet surveillance - article 36 (4) Alerts relating to objects that are misappropriated, lost, stolen and which may be sought for the purposes of seizure or for use as evidence (e.g. firearms, passports etc) - article 38 (2) (a) (e) and (f)	All criminal activity
Information made available	Vehicle keeper data	That a vehicle has been stolen or is wanted as evidence (e.g. to be searched because it is suspected of being used to support criminal activity). That there has been a hit on an object on which a discreet surveillance marker has been placed.	Vehicle registration data including keeper details
Main differences	Focus is on getting hold of information about a vehicle e.g. keeper	Focus is a) on finding out whether vehicle is wanted (e.g. stolen) and enabling police to stop and seize said vehicle and b) getting reports back on vehicles on which discreet surveillance markers have been placed	Focus is on getting hold of information about a vehicle e.g. keeper and VIN number
Timeframes	In 10 seconds or as agreed by batch	Information uploaded in real time. Not a	In 10 seconds

		request based system, so no 'reply' time limits	
Territorial Scope	All EEA have implemented or will need to implement	All EU Member States plus Switzerland, Norway, Iceland and Liechtenstein.	All EU Member States plus Norway, Iceland Switzerland and Liechtenstein

Safeguards

Data Protection within Prüm

Chapter 6 of Council Decision 2008/615/JHA sets out the Data Protection Framework under which exchange may take place.

Article 25(1) requires Member States to guarantee a level of protection at least equal to that resulting from the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Convention 108) and its Additional Protocol of 8 November 2001. Article 25(2) states that a Member State may only exchange information if it has passed a data protection evaluation.

Article 26 concerns purpose limitation. The processing of data by the receiving Member State shall be permitted solely for the purposes for which the data have been supplied. These purposes are further defined as:

> (a) Establishing whether the compared DNA profiles or dactyloscopic data match;
> (b) Preparing and submitting a police or judicial request for legal assistance in compliance with national law if those data match; and
> (c) Recording within the meaning of Article 30.

Data supplied must be deleted unless it is required for the purposes set out in points b and c above. This means that profiles, fingerprints and license plate number/VINs cannot be stored on the receiving country's systems.

Article 28 sets out accuracy, current relevance and storage time of data requirements. This includes a requirement to notify a Member State if data supplied is incorrect or should not have been supplied. Any incorrect data should be corrected. If the accuracy or inaccuracy of data cannot be ascertained, the data are to be flagged. Member States cannot store data for longer than the law of the sending Member State permits.

Article 29 requires Member States to have technical and organisational systems to ensure data is protected and kept securely.

Article 30 sets out requirements for logging and recording, including what should be recorded, who should be authorised to access any data, and time limits for retention of the logging requirements. In Article 30(5), the Decision sets out that that the independent data protection authorities in each Member State (for the UK this would be the Information Commissioner's Office and Biometric Commissioner) should carry out random checks on the lawfulness of supply.

Article 31 sets out data subject rights. Data must be supplied comprehensibly and without unacceptable delays, on the data processed in respect of his person, the origin of the data, the recipient or groups of recipients, the intended purpose of the processing and, where required by national law, the legal basis for the processing.

Proportionality

Release of Information

One of the concerns expressed on Prüm is that DNA and, to a lesser extent, fingerprints will be sent for comparison even though the offence from which they were recovered is a minor one. Prüm does not permit Member States to reject a request on the grounds of proportionality; there is simply no technical way of stopping a request being made. However it is possible, in the event of a hit, for a Member State to choose not to send personal data if the crime abroad is not sufficiently serious i.e. to apply proportionality bar in respect of the offence being investigated.

Minors

The Government has decided to add an additional proportionality safeguard to follow up requests for personal data following a verified hit on minors on the databases. It will be necessary for the requesting Member State to use a Letter of Request via Mutual Legal Assistance channels which involve additional hurdles.

European Arrest Warrant (EAW)

The impact of Proportionality considerations in EAW cases may result further down the line in the investigation into a verified match by a Member State.

The Anti-social Behaviour, Crime and Policing Act 2014 introduced a number of reforms to the operation of the European Arrest Warrant in Part 1 of the Extradition Act 2003. The changes include the introduction of a proportionality test which came into force on 23 July 2014. As a result, judges considering EAW cases are required to decide whether extradition would be disproportionate and, if so, must order the person's discharge. In making such decisions, judges must take into account the seriousness of the alleged conduct, the likely penalty and the possibility of the issuing state taking less coercive measures than extradition, for example, by issuing a court summons.

The proportionality test is complemented by an administrative proportionality check, carried out by the NCA, for each incoming accusation EAW as part of the certification process where the person has been accused of a crime, rather than convicted of a crime. The purpose of the check is to identify those EAWs which are likely to be discharged by the court on proportionality grounds. In deciding whether to refuse to certify an EAW on proportionality grounds, the NCA must follow guidance issued by the Lord Chief Justice issued with the concurrence of his counterparts in Scotland and Northern Ireland. The judiciary follow the same guidance, although it is not strictly binding upon them. The guidance sets out categories of offences for which, unless there are exceptional circumstances, judges should generally determine that extradition would be disproportionate. The following categories, together with examples, are included in the guidance:

- Minor theft - (not robbery/ burglary or theft from the person) where the theft is of a low monetary value and there is a low impact on the victim or indirect harm to

others, for example: theft of an item of food from a supermarket; theft of a small amount of scrap metal from company premises; theft of a very small sum of money.

- Minor road traffic, driving and related offences where no injury, loss or damage was incurred to any person or property, for example: driving whilst using a mobile phone; use of a bicycle whilst intoxicated.
- Minor criminal damage, (other than by fire) for example, breaking a window.

Two stage process

For DNA and fingerprints, Prüm is a two-stage process. The initial stage is a hit/no-hit process in which anonymous or pseudonymised data is exchanged. The hit reply does not contain details of the profile hit against: instead, for DNA, it will contain the individual values which have matched, for fingerprints it will be the image matched against. In both cases these will be accompanied by a reference number. It is not possible from the information supplied with a hit for the requesting Member State, on its own, to find out the person to whom the hit refers.

The second stage process involves the original requesting Member State sending the reference number to a national point of contact and asking for personal details in relation to the person hit against. It is at this point that demographic data is exchanged and the person against whom there has been a match is identified.

Adventitious Matching Study Recommendations Response

Prüm requires Member States to report, as hits, matches of six or more loci. As set out earlier, this causes a well known problem concerning adventitious or false positive matches. In simple terms, for a match using relatively few loci (6 and 7) the chance of a hit being a true one is lowered, but possible, i.e. the hit is a result of chance rather than any genuine connection. This means that a 6 or 7 loci hit cannot be relied upon. More adventitious matches occur with 6 loci (approx. 26-38% true matches) and 7 loci (approx. 82-94% true matches). With 8 loci and above, c.98% or more of the matches observed will be true matches

Prüm requires the initial hit to be returned for a 6 loci hit or more. It does *not* require personal data to be exchanged in relation to that hit. It is possible for the UK, as has been the case with other countries, to provide personal data only if the number of loci is sufficient for there to be a very high probability indeed that the hit is a true one. For the UK this would be 10 loci, i.e. we would only provide personal data if there was a 10 loci or more match. In doing this, the UK would be taking the same route as almost all countries which currently routinely discard 6 or 7 loci hits in relation to profiles they have sent and refuse to provide personal details in relation to 6 or 7 loci hits. The larger number of profiles held on the UK's National DNA Database requires a higher number of loci to match for the hit to be guaranteed to be a true one.

Therefore, as set out above, should the UK rejoin Prüm, the Government has decided it would adopt higher standards on DNA loci than the minimum stipulated in the Prüm decisions and accept the recommendation of the PFS study that:

- Only crime scene profiles with more than 8 loci would be shared with other Member States on the UK Prüm exchange.
- The UK would share its subject profiles with other Member States but demographic data for subjects would only be 'routinely' shared following the match of 10 or more loci.

Forensic Standards

Quality standards in forensic science are integral to the criminal justice system. Framework Decision 2009/905/JHA provides assurance of the technical competence of a Member State laboratory to undertake specified analysis and also reviews particular aspects relevant to the Criminal Justice System, for example, continuity of evidence, management of case files and storage of exhibits. The accreditation element determines the competence of staff, the validity and suitability of methods, the appropriateness of equipment and facilities, and the ongoing assurance and confidence in outcomes through internal quality control.

Eurodac Access

In a workshop hosted by the Home Office on 17 July 2015, Liberty expressed concern about Prüm enabling access to databases such as Eurodac for law enforcement purposes.

The decision to allow Law Enforcement Authorities access to Eurodac was prompted by decisions such as The Hague Programme which called for the improvement of access to existing data filing systems in the Union and The Stockholm Programme which called for well targeted data collection and a development of information exchange and its tools that is driven by law enforcement needs.

Consideration was given to the Article 8 'right to privacy'. The Commission outlines in its Communication to the Council and the European Parliament of 24 November 2005[70] that authorities responsible for internal security could have access to Eurodac in well defined cases, when there is a substantiated suspicion that the perpetrator of a terrorist or other serious criminal offence has applied for international protection. In that Communication, the Commission also found that the proportionality principle requires that Eurodac be queried for such purposes only if there is an overriding public security concern. The act committed by the person to be identified must be so reprehensible that it justifies querying a database that registers persons with a clean criminal record, and it concluded that the threshold for authorities responsible for internal security to query Eurodac must therefore always be significantly higher than the threshold for querying criminal databases.

For this reason, the definition of an offence which can result in a search of Eurodac is as follows:

- 'terrorist offences' means the offences under national law which correspond or are equivalent to those referred to in Articles 1 to 4 of Framework Decision 2002/475/JHA;

[70] on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs

- ‘serious criminal offences' means the forms of crime which correspond, or are equivalent to those referred to in Article 2(2) of Framework Decision 2002/584/JHA, if they are punishable under national law by a custodial sentence or a detention order for a maximum period of at least three years.

The article which sets out the conditions where a Eurodac search would be permitted for law enforcement purposes is Article 20 of Regulation 603/2013 Conditions for access to Eurodac by designated authorities. This prevents searches of Eurodac unless other relevant databases have been searched first and provided the following conditions are met:

(a) the comparison is necessary for the purpose of the prevention, detection or investigation of terrorist offences or of other serious criminal offences, which means that there is an overriding public security concern which makes the searching of the database proportionate;
(b) the comparison is necessary in a specific case (i.e. systematic comparisons shall not be carried out); and
(c) there are reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question. Such reasonable grounds exist in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls in a category covered by this Regulation.

If Parliament votes to rejoin Prüm, it would offer UK law enforcement the opportunity to access Eurodac for very serious cases. This would not give access to the Visa Information System (VIS)[71] for visa applicants and would not prejudice any claim for international protection ongoing should a match be found with a Eurodac fingerprint set. This provision is set out in recital (9) of the Regulation which states:

“The powers granted to law enforcement authorities to access Eurodac should be without prejudice to the right of an applicant for international protection to have his or her application processed in due course in accordance with the relevant law. Furthermore, any subsequent follow-up after obtaining a hit from Eurodac should also be without prejudice to that right.”

Another condition which further protects those whose fingerprints are held on Eurodac is that they can only be held; (i) for asylum-seekers, until documentation has been issued or citizenship granted; and (ii) for irregular migrants, for 18 months.

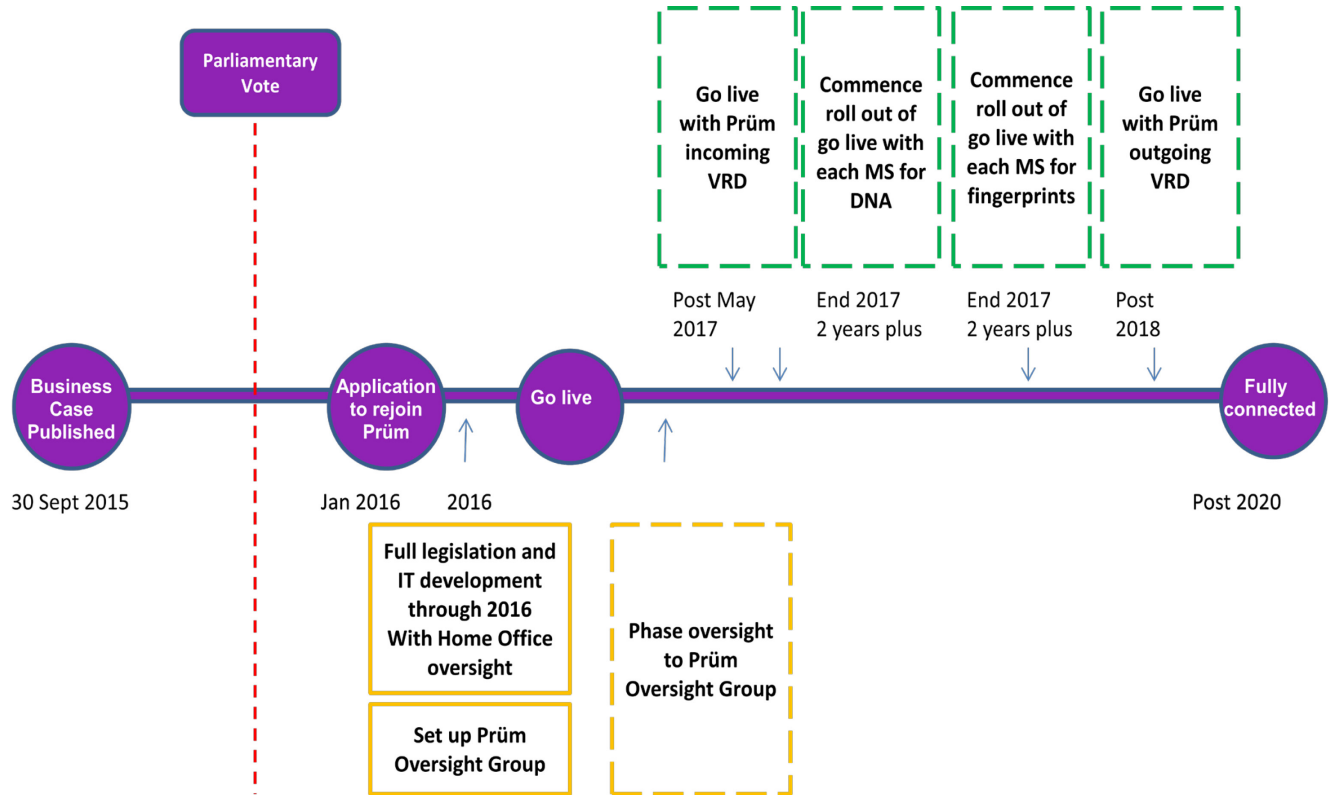
[71] http://ec.europa.eu/dgs/home-affairs/e-library/docc/vis_factsheet

Prüm Implementation

Timeline

The following section sets out the high level solutions for implementing Prüm should Parliament vote to rejoin. The Prüm application process and the development requirements for the UK solution mean that it would likely be 2017 at the earliest before any UK Prüm connections could be made. Indeed it may be later.

Figure 5 Implementation Timescale



Governance

If Parliament votes to rejoin, Prüm governance would be set up through a Prüm Oversight Group, with membership from at least the NCA, the National Police Chiefs' Council (fingerprints, DNA and vehicle leads), Police Scotland, Police Service Northern Ireland, the Home Office, Department for Transport, Scottish Government, Department of Justice Northern Ireland and the National DNA Database Delivery Unit.

The Information Commissioner and Biometric Commissioner will be responsible for auditing UK compliance with Prüm as set out above. The National DNA Strategy Board will continue to retain oversight of international DNA exchange.

IT

DNA

In the event of Parliament voting to rejoin Prüm, there would be a requirement to deliver a database connection to NDNAD and the Biometric Service Gateway (BSG which is due to be in place by June 2016). See figure 6.

The strategic solution would mean building Prüm capability into the strategic Home Office Biometrics (HOB) solution which would encompass the evolution of the current NDNAD. An interface with the PNC would be in place to ensure that only the required records are included in the collection searchable by Member States. A workflow engine would ensure that DNA profiles and stains are progressed through national searches and onto Prüm as required. A common user interface would be provided to users in the national control units to manage national, counter terrorism and Prüm records, searches and results. The solution would build on the HOB platform (which would provide hosting, platform services and system management and monitoring capabilities).

The rough order of magnitude is set out in the cost section and would be developed in full in the event of a positive vote in Parliament. The solution would require the creation of a central Prüm Review Team to validate Prüm DNA hits. Costs for the review function are set out alongside the IT costs.

Fingerprints

Post 2017, there would be a requirement to deliver a fingerprint solution using IDENT1 and the Biometric Services Gateway[72].

It is envisaged that this would be a phased implementation.

Phase 1

Outbound
Assuming all of the approvals required were in place and implementation could go ahead; an initial Prüm solution would be deployed that contains a lower level of automation and technical change than the ultimate solution. See figure 7.

This initial implementation would only connect to two or three other Prüm countries and would deploy the essential technical building blocks of a Prüm fingerprint exchange solution whilst delaying the extended timescales, cost and technical complexity required for a full solution until the business process is proven. For example, the functionality required to manage search quotas in this initial deployment would be manually provided by the NCA undertaking the Gatekeeper role rather than automated through the IT solution.

[72] As set out above, the BSG will not be in place until June 2016.

The gatekeeper function would ensure that the number of outbound requests for each fingerprint type would not exceed the quotas provided. As a central point of contact, the gatekeeper would, as is already the case in other countries, be able to negotiate for one-off capacity increases with other countries or accept one off increases in incoming capacity. Each Member State has chosen to implement Prüm fingerprint functionality incrementally, country by country; the UK would do the same. It is believed that a service working nine hours a day five days a week (9/5) would be sufficient. Costs for the gatekeeper function are set out alongside the IT costs.

Inbound
By contrast incoming Prüm transactions are relatively easy to manage and there is only one relevant technical solution option. The proposed high level technical solution for incoming Prüm transactions from other Prüm countries is illustrated below (see figure 8). This solution would be deployed at Phase 1 implementation. It is not expected to materially change for Phase 2 implementation.

Phase 2
This initial implementation would be followed by deployment of a full solution with a greater level of automation, which could support the wider rollout of connections to other Prüm countries. The full solution would require further technical change but build on the technical solution already deployed initially so would encompass spend already made. The rough order of magnitude is set out in the cost section below.

Vehicle Registration Data

The Government are required to allow Member States to access Vehicle Registration Data held in the UK so as to implement a new Directive on Cross Border Enforcement of road safety traffic offences, for incoming requests from Member States as a minimum, by May 2017 (see figure 9). However, the Government recognises the importance of reciprocity in this field and is actively considering how to enable outgoing requests from the UK to Member States to ensure that Member State registered vehicles are subject to the same road traffic offence enforcement that UK registered drivers are whilst driving in Member States.

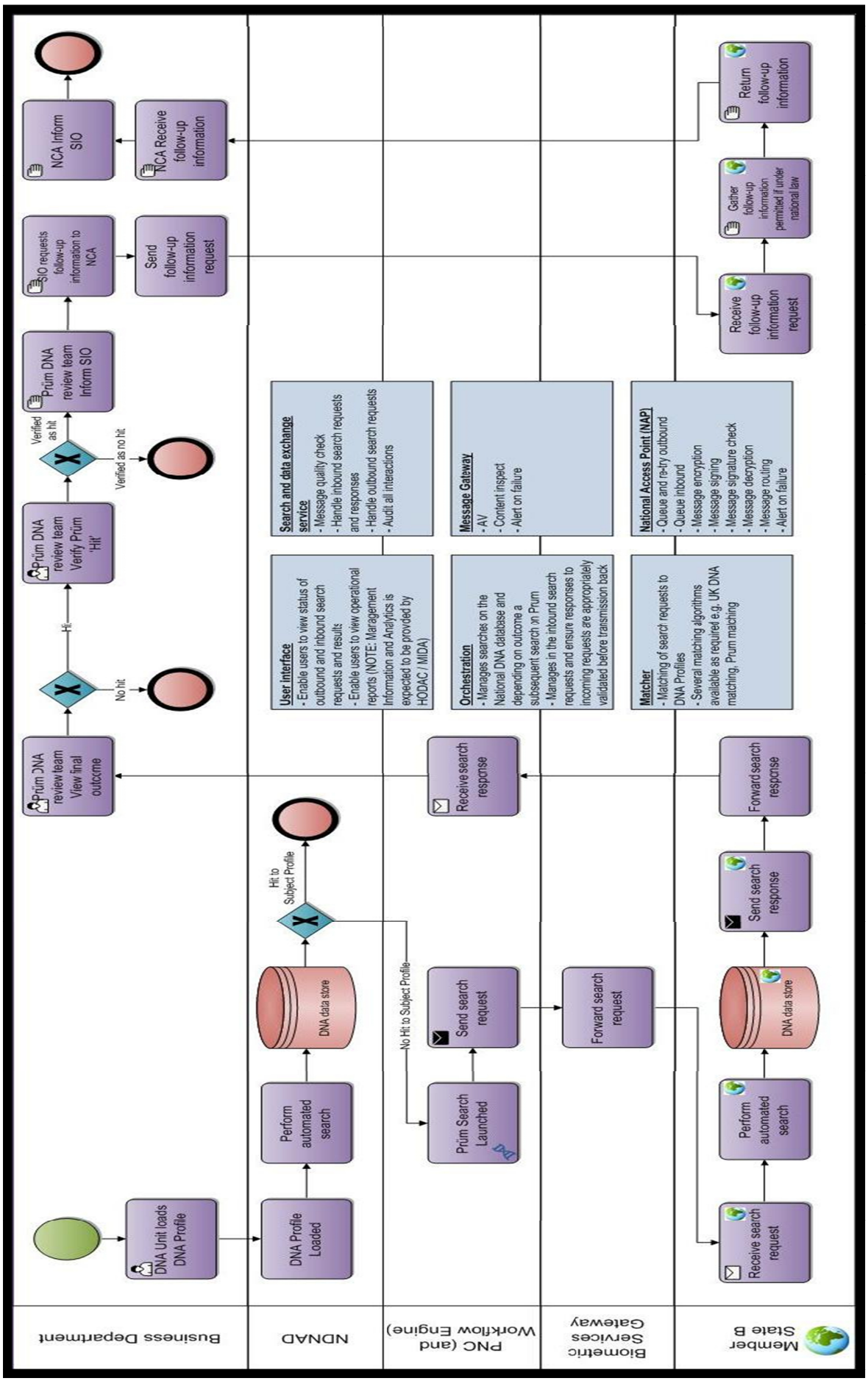


Figure 6 Strategic DNA Solution

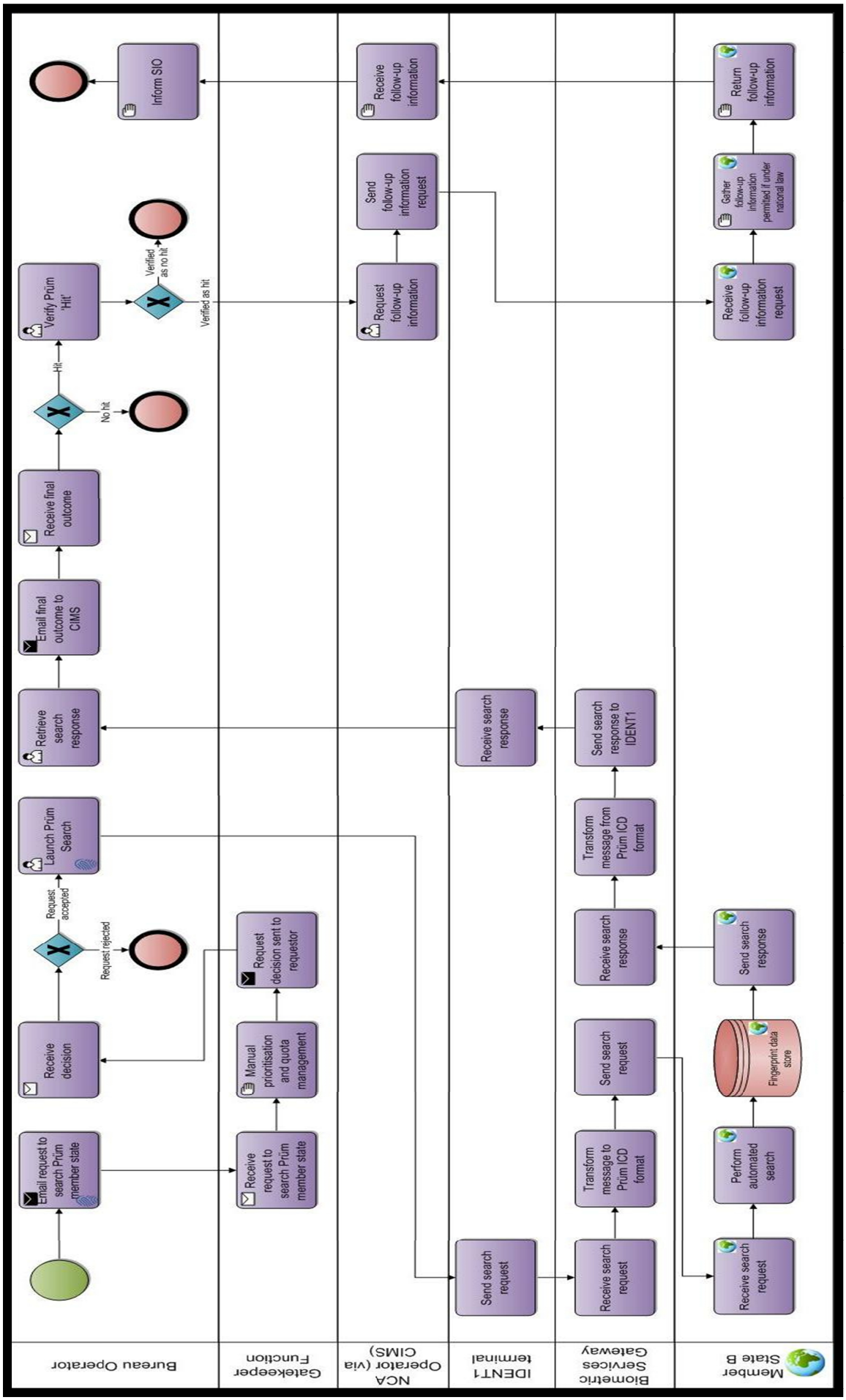


Figure 7 Fingerprints Outbound

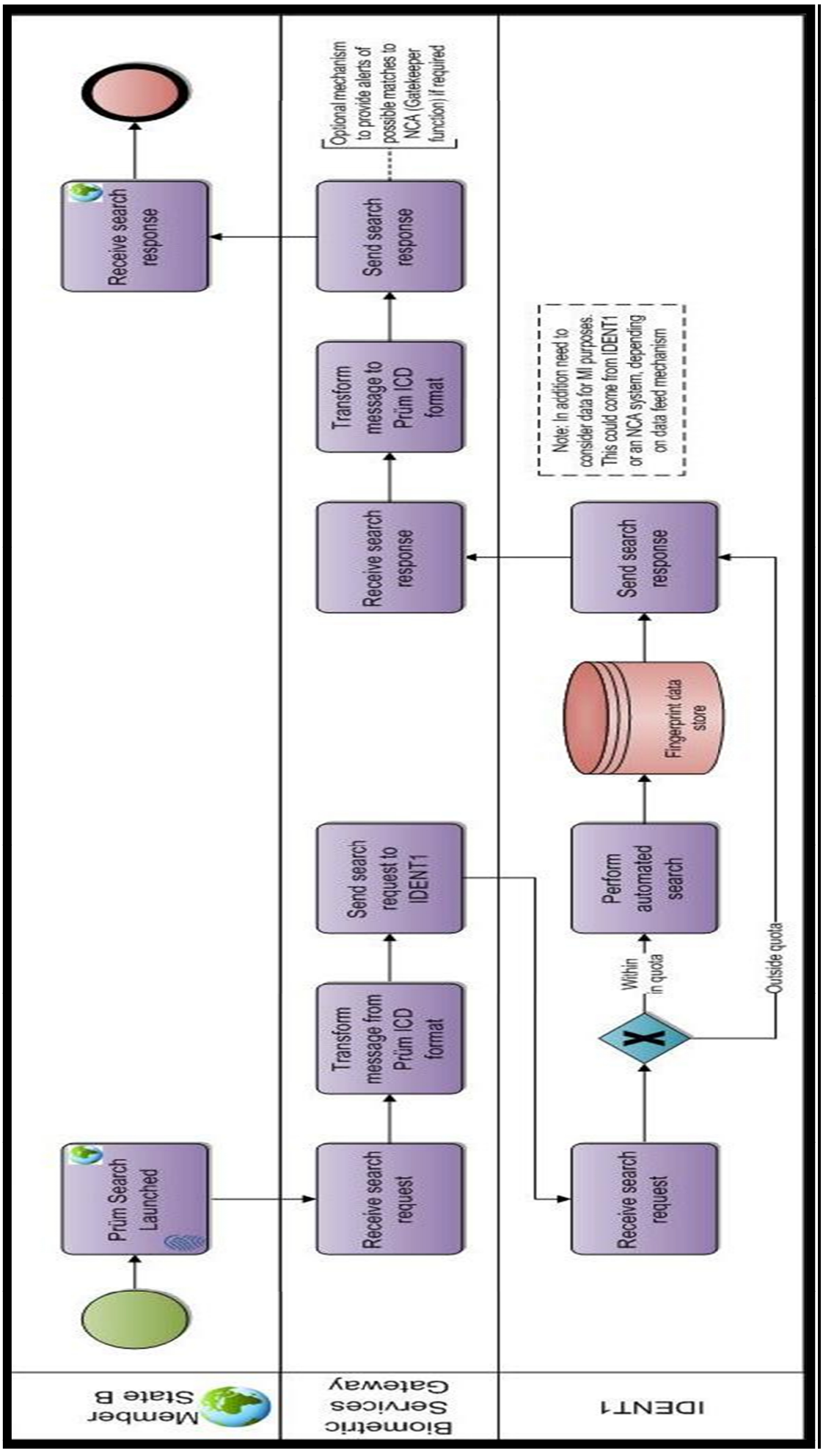


Figure 8 Fingerprints Inbound

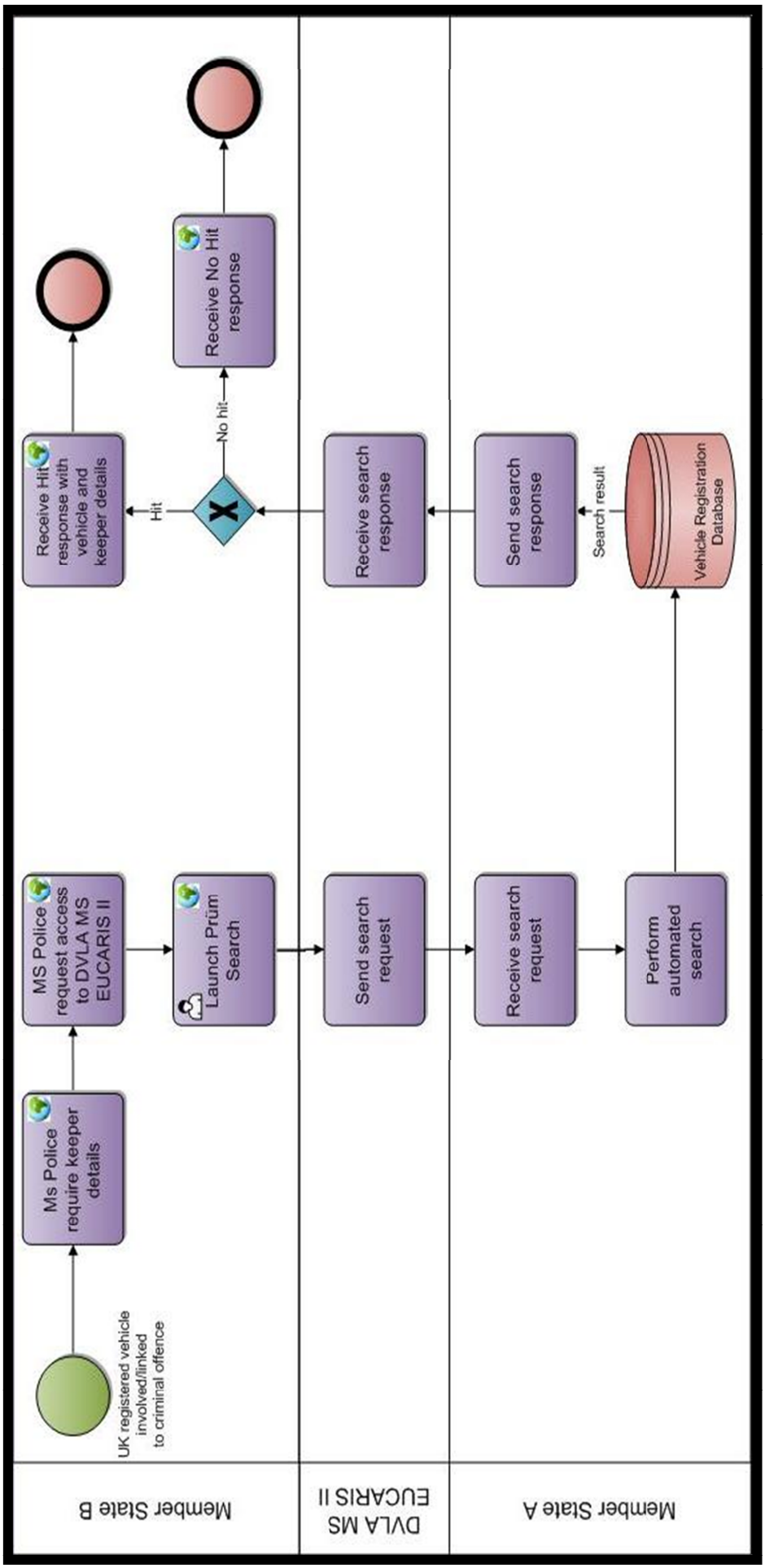


Figure 9 Inbound Member State searching UK held VRD

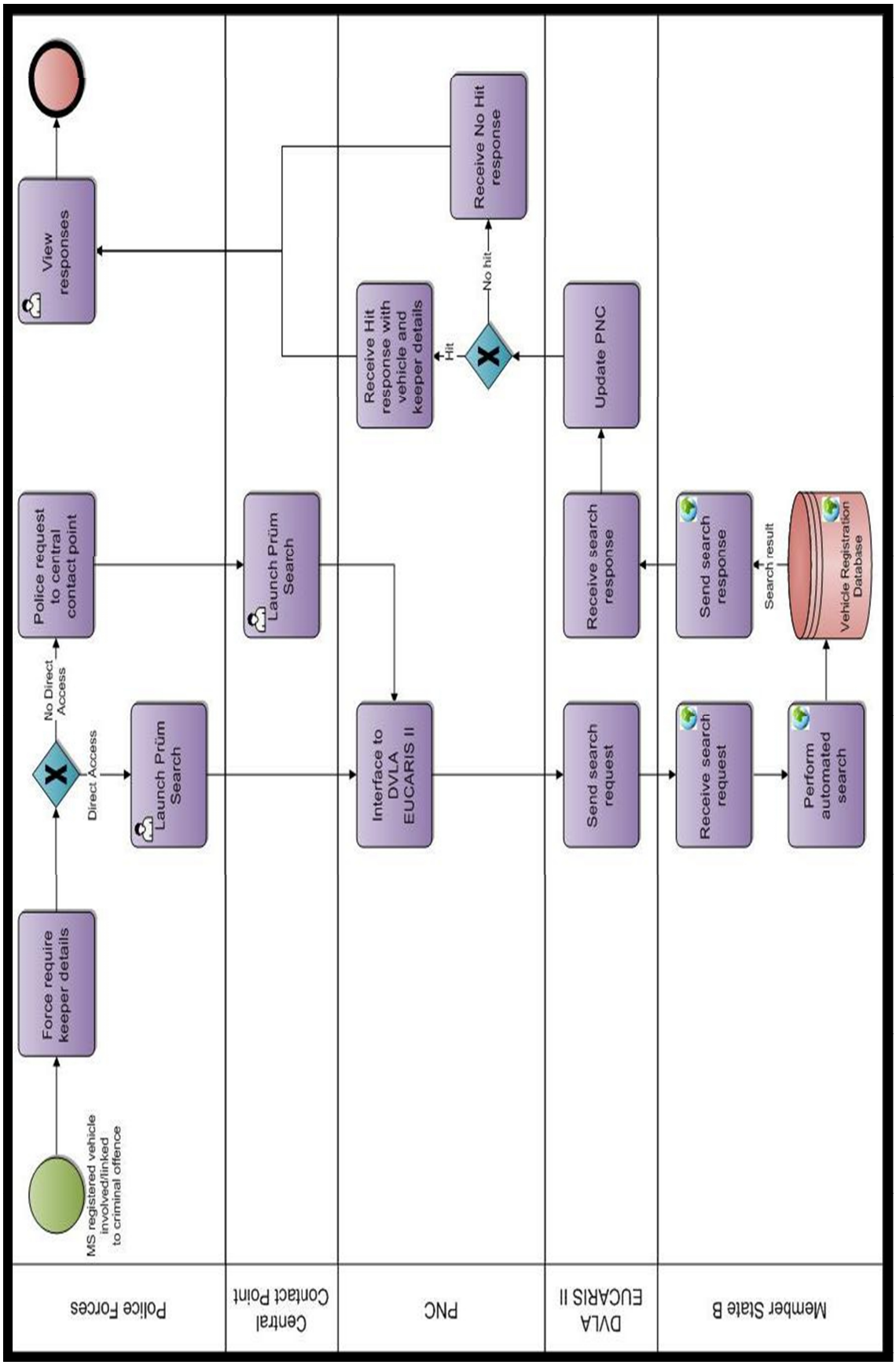


Figure 10 UK searching Member State held VRD

Costs

Table 14 Costs

	IT Project Costs	IT Run Costs	Business Operational Costs
DNA Strategic HOB solution	£2.7Mn	£0.9Mn	£0.07Mn- £0.11Mn
Fingerprints HOB Strategic Solution Phase 1	£4Mn	£0.8Mn	£0.06-£0.08Mn
Fingerprints HOB Strategic Solution Phase 2	£1.8Mn	£0.55Mn	£0.3Mn
On boarding costs	£1Mn	N/A	N/A
VRD HMG Strategic Solution	£0.5Mn	£0.75Mn	N/A
Total	**£10Mn**	**£3Mn**	**£0.43Mn-£0.49Mn**
	Total IT Cost £13Mn		

Assumptions

1. Prüm fingerprint and DNA projects are run within HOB, an established governance structure and supporting assurance/PMO is in place.
2. Costs have been estimated based on high level requirements and based on an initial assessment of the complexity and size of each component. Further analysis should be undertaken to confirm costs. Quotes or ROMs have not been requested from any suppliers.
3. Discussions with Member States on the system sizing should take place to validate assumptions
4. The BSG has already been built and Prüm is a feature of it
5. Assumes that the PNC can be developed to provide conviction status for DNA and fingerprints
6. DNA: Business operational costs have been estimated based on high level requirements and based on an initial assessment of potential DNA matches of new crime scene stain profiles per year at the high end of 5% of 40,000. This equates to a 2,000 hit rate per year when at full connectivity.
7. IDENT1 capacity increase not required
8. IDENT1 service management costs are not uplifted as a result of introducing this service

9. Foreign National Offenders Stage 2 work is complete prior to Prüm fingerprint starting
10. Requirement to establish a staffed fingerprint gatekeeper post for filtering and sending UK Prüm outgoing search requests in line with quota system. This model is based on an assumption that the gatekeeper process will start manually and, as the UK connects with more countries, greater automation will be developed requiring less manual intervention. Volumes can be managed up to the quota levels so that work can be set within resources. This will additionally enable baseline data to be developed which is currently unavailable.
11. That Government implement the Directive on cross border enforcement (set out in Option 1) of road safety traffic offences as required, to allow Member States to access Vehicle Registration Data, for both incoming and outgoing searches. Prüm would complement these developments, by extending the level of offences for which VRD checks can be made. If the system is built to enable outgoing searches from the UK to Member States, Prüm requests would reuse much of the same infrastructure.
12. That the UK VRD Prüm development mirrors the CBE development and build upon it to minimise costs.

Further Downstream Operational Running Costs

The downstream costs to police forces of verification of fingerprint matches will ramp up slowly with small volumes and will be dispersed across forces. As connections develop it will be possible to work up estimates on capacity in a controlled environment should the UK rejoin Prüm. This also applies for the rest of Prüm. There would be downstream costs to the police, Crown Prosecution Service, Crown Office (in Scotland), Public Prosecution Service for Northern Ireland, Courts and the NCA. There would be post Prüm follow up via requests which would be reflected in an increased volume of use of secure police or mutual legal assistance channels (in accordance with well-established procedures). It is estimated that each additional inbound extradition would cost the Criminal Justice System £29,000 and each outbound one £13,000[73]. However it is not the case that every hit will lead to an extradition and a prosecution. The initial hit provides investigative information for law enforcement agencies. It is also necessary to note that there is no clear chain of causality between a hit and a court case. For example, DNA is in most cases not relied upon as the sole evidence in court so proving that a DNA hit caused a prosecution is not possible. The volumes would also be subject to ever diminishing returns as cases progress through the system for a variety of reasons[74]. This makes it very difficult to estimate the likely number of prosecutions. However, the ability of the UK to control the connections to Prüm would enable this to be managed within capacity. In addition, twenty-one Member States currently operate Prüm, yet none show any evidence of Prüm overburdening their police or courts systems.

[73] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/326699/41670_Cm_8897_Print_Ready.pdf

[74] Such as, the crime has already been solved by other means; the match turns out not to be relevant to the investigation; the match is true, but expected sentence is less than 6 months and person is abroad so CPS do not seek extradition; person match to a single crime scene profile/mark occurs in more than one country, i.e. no one to one equivalence between a hit and an person

Legislation

There is no formal obligation on the UK to transpose Council Decisions 2008/615/JHA and 2008/616/JHA into domestic law: the UK is only required to implement them. On the other hand, the UK is obliged to transpose Council Framework Decision 2009/905/JHA.

Council Decisions 2008/615/JHA and 2008/616/JHA
Our view is that there is nothing within Council Decisions 2008/615/JHA and 2008/616/JHA that needs to be transposed into domestic law.

Safeguards
It may, nevertheless, be considered desirable to include the following in domestic legislation.

First, legislation could specify that when other Member States conduct searches through Prüm against the UK's DNA and fingerprint databases, those searches will not be run across the DNA or fingerprints of those who have not been convicted.

Second, the following safeguards could be put in place before personal data is sent to another Member State following a hit on the UK's DNA database: (i) in the event of a person-to-person hit (i.e. a hit that just confirms the identity of an individual, who has already been identified in another Member State), the UK will request the individual's fingerprints and, if those fingerprints are provided, use the fingerprints to confirm their identity; (ii) the UK will not provide personal data unless the DNA hit is sufficiently accurate (i.e. is accurate to 10 loci or more); and (iii) in the event of a hit against a person under 18 years old, the UK can only provide personal data if the Member State makes a request for the information using a formal Letter of Request via mutual legal assistance channels

Finally, safeguard (iii) in relation to persons under 18 years old could also be applied to hits against the UK's fingerprint database.

Draft legislation to implement these safeguards is at Annex J.

Council Framework Decision 2009/905/JHA
Legislation to implement Council Framework Decision 2009/905/JHA is set out at Annex J.

Nature of the legislation
Legislation could be adopted by way of secondary legislation under s. 2(2) of the European Communities Act 1972 or by primary legislation.

There may also need to be further legislation or amendments to the draft legislation to fully capture the safeguards and forensic service provider requirements set out above in relation to Northern Ireland and Scotland.

Option 3: Alternatives to Prüm

Description of Option

There are two possible options that would, if negotiable, allow the UK to adopt Prüm-style arrangements with other Member States other than through opting in to the Prüm Decisions.

i) an international agreement with the EU incorporating some or all of the provisions of the Prüm Decisions (similar to the arrangements Norway and Iceland have with the EU on Prüm); and

ii) bilateral agreements between the UK and individual Member States.

International Agreement

Consideration has been given as to whether it would be possible to negotiate an international agreement with the EU that would allow the UK to participate in Prüm without becoming subject to the CJEU's jurisdiction. It would not, in practice, be possible.

To date, Denmark is the only Member State with which EU has concluded an international agreement in the field of JHA. Denmark has agreements (or treaties) with the EU concerning:

- the Dublin II Regulation on asylum and Eurodac (from 2006);
- the Brussels I Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (from 2005); and,
- the Regulation on the service of judicial and extrajudicial documents in civil or commercial matters (from 2005).

Some have argued that the government could therefore pursue this approach. However, the comparison is a false one. Unlike the UK, Denmark is currently prohibited from participating in JHA measures as a result of Protocol 22. Therefore, unless Denmark concludes an international agreement with the EU it has no legal alternative to ensuring their participation in JHA measures. Protocol 36 allows the UK to rejoin measures it has previously opted out of and the European Commission argues that this provides adequate provision to mean that a third country agreement is unnecessary, both legally and politically. In addition, Article 2(3) of Council Decision 2014/836/EU is explicit that "*the United Kingdom shall decide by 31 December 2015 whether to notify the Council of its wish to participate in the Prüm Decisions in accordance with Article 10(5) of Protocol No 36*". Therefore, concluding an international agreement allowing UK participation in Prüm would require the government to repay €1.5m, as the terms of Council Decision 2014/836/EU would not have been complied with.

Furthermore, all agreements concluded to date require Denmark to submit to CJEU jurisdiction for both interpretation and to ensure compliance. This was a red line for

the Commission and Council during the negotiations with Denmark. Therefore, even if were possible to open negotiations on an international agreement with the EU, precedent shows that the government would be required to accept CJEU jurisdiction in order to conclude such a deal.

In procedural terms, an international agreement with the EU would need to be proposed by the Commission. As noted above, the Commission argues that the UK can rejoin JHA measures through the process set out in Protocol 36 and can point to Article 2(3) of Council Decision 2014/836/EU as adding extra weight to that. There is no precedent for an international agreement between the EU and a Member State that already has the ability to participate in EU measures by specific means. Consequently, the Commission would be highly unlikely to propose such an international agreement.

Following its proposal an international agreement requires the consent of the European Parliament and a qualified majority of other Member States to support it. Indications are that the vast majority of other Member States would take a similar view to the Commission, meaning it is improbable that a qualified majority could be achieved. Finally, the views of the European Parliament on this issue are unknown but they have, historically, been supportive of a consistent approach to the application of EU laws and would be unlikely to look favourably on an international agreement in this context, especially where an alternative legal route to achieving the same outcome exists.

Bilateral Agreements with Member States

This would involve having bilateral Prüm-style agreements with certain other Member States. Such agreements would require the consent of those other Member States and they would need to decide whether they were competent to enter such agreements. The cost of implementation would be the same as implementing Prüm and the process would be similar.

While the UK has already entered bilateral memoranda of understanding (***MoUs***) with Member States to exchange DNA, these agreements are time limited and have been entered into by four Member States in the context of the UK's Business and Implementation Case.

It would be possible for the UK to add conditions to the agreement/bilaterals that are different to Prüm. The UK would retain the ability to unilaterally denounce the agreement/bilateral. This would apply equally to the other Member States.

It may not be legally possible to arrange a co-operation agreement or bilaterals outside of Prüm with the EU or Member States. Even if it were legally possible, it may not be possible to reach a co-operation agreement or bilaterals as the EU or Member States may be unwilling to participate with the UK outside of Prüm.[75]

Any such agreements will remain subject to the jurisdiction of the CJEU.

[75] Anecdotal evidence from police has already suggested an unwillingness of MS to enter bilaterals with the UK since Prüm went live.

Glossary

Term	Definition
ACRO	ACRO Criminal Records Office
Adventitious match	DNA profiles from two individuals, who are not identical twins, which match by chance.
AFIS	Automated Fingerprint Identification System
Allele	Alternative forms of a DNA sequence at a particular locus
BSG	Biometric Services Gateway
CBE	Cross Border Enforcement Directive
CJEU	Court of Justice of the European Union
CODIS	Combined DNA INDEX System
CPIA	Criminal Procedure and Investigation Act 1996 (as amended)
Council Decision	Binding EU legal instrument with direct effect
DAPIX	European Union Working Group on and Data Protection and Information Exchange
DNA	Deoxyribonucleic acid
DNA17	DNA multiplex that contains all the loci specified by ENFSI
DNA profile	Any information derived from a DNA sample
DNA sample	Any material that has come from a human body and consists of or includes human cells
DVA	Driver and Vehicle Agency (Northern Ireland)
DVLA	Drivers and Vehicle Licensing Agency
EAW	European Arrest Warrant
ECRIS	European Criminal Records Information System
EIO	European Investigation Order
ENFSI	The DNA Working Group of the European Network of Forensic Science Institutes
EPGs	Electropherograms
ESO	European Supervision Order
ESS	European Standard Set (of loci)
EU	European Union
EUCARIS	European Car and Driving License Information System
Eurodac	European Dactyloscopy, the European fingerprint database for identifying asylum seekers and irregular border crossers
FP	Fingerprint
Framework Decision	An EU legislative act that does not have direct effect but required transposition into domestic law
FNO	Foreign National Offender
FSP	Forensic Science Provider
HOB	Home Office Biometrics
I 24/7	Interpol's global police communication system
ICMP	International Commission on Missing Persons
IDENT1	The UK's central national fingerprint database
ISEC	EU finding stream on the Prevention of and Fight against Crime

JHA	Justice and Home Affairs
LEA	Law Enforcement Agency
Locus (pl. loci)	Specific location of a DNA sequence on a chromosome; for forensic analysis it refers to areas that vary between individuals
LP	Latent Palmprint
LT	Latent
MLA	Mutual Legal Assistance
MO	Modus Operandi
MoU	Memorandum of Understanding
MPS	Metropolitan Police Service
MS	Member State
Multiplex	DNA system that simultaneously analyses several loci in a single test
NCA	National Crime Agency
NCP	National Contact Point
NDNAD	National DNA Database
NDU	National DNA Database Delivery Unit (UK)
NIST	National Institute of Standards and Technology
NFO	National Fingerprint Office
PoFA	Protection of Freedoms Act 2012
PFS	Principal Forensic Services Ltd
PP	Palm print
Prüm Decisions	EU Council Decision 2008/615/JHA (Chapter 2) and its implementing decision, 2008/616/JHA of 23 June 2008 (in conjunction with Council Framework Decision 2009/905/JHA) are commonly referred to as the Prüm Decisions
SCJS	Sustainable Criminal Justice Solutions
SGMPlus®	Second Generation Multiplex Plus (standard UK multiplex from1999 2014)
SIENA	Secure Information Exchange Network Application
SIRENE	Supplementary Information Request at the National Point of Entry
SIS	Schengen Information System
STESTA	Secure Trans European Services for Telematics
TP	Tenprint
UIPDE	UK Prüm DNA Evaluation
UKPFE	UK Prüm Fingerprint Evaluation
UKNCB	UK Interpol National Central Bureau (part of NCA UKICB)
UMF2	Universal Messaging Format 2nd version
VIN	Vehicle Identification Number
VIS	Visa Information System
VISOR	Violent and Sex Offender register
VRD	Vehicle Registration Data
Wild card	An undesignated placeholder included where the presence of an allele is uncertain but needs to be considered

III

(Acts adopted under the EU Treaty)

ACTS ADOPTED UNDER TITLE VI OF THE EU TREATY

COUNCIL DECISION 2008/615/JHA

of 23 June 2008

on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 30(1)(a) and (b), Article 31(1)(a), Article 32 and Article 34(2)(c) thereof,

Having regard to the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden,

Having regard to the Opinion of the European Parliament [1],

Whereas:

(1) Following the entry into force of the Treaty between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration hereinafter (Prüm Treaty), this initiative is submitted, in consultation with the European Commission, in compliance with the provisions of the Treaty on European Union, with the aim of incorporating the substance of the provisions of the Prüm Treaty into the legal framework of the European Union.

(2) The conclusions of the European Council meeting in Tampere in October 1999 confirmed the need for improved exchange of information between the competent authorities of the Member States for the purpose of detecting and investigating offences.

(3) In the Hague Programme for strengthening freedom, security and justice in the European Union of November 2004, the European Council set forth its conviction that for that purpose an innovative approach to the cross-border exchange of law enforcement information was needed.

(4) The European Council accordingly stated that the exchange of such information should comply with the conditions applying to the principle of availability. This means that a law enforcement officer in one Member State of the Union who needs information in order to carry out his duties can obtain it from another Member State and that the law enforcement authorities in the Member State that holds this information will make it available for the declared purpose, taking account of the needs of investigations pending in that Member State.

(5) The European Council set 1 January 2008 as the deadline for achieving this objective in the Hague Programme.

(6) Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2] already lays down rules whereby the Member States' law enforcement authorities may exchange existing information and intelligence expeditiously and effectively for the purpose of carrying out criminal investigations or criminal intelligence operations.

(7) The Hague Programme for strengthening freedom, security and justice states also that full use should be made of new technology and that there should also be reciprocal access to national databases, while stipulating that new centralised European databases should be created only on the basis of studies that have shown their added value.

[1] Opinion of 10 June 2007 (not yet published in the Official Journal).

[2] OJ L 386, 29.12.2006, p. 89.

(8) For effective international cooperation it is of fundamental importance that precise information can be exchanged swiftly and efficiently. The aim is to introduce procedures for promoting fast, efficient and inexpensive means of data exchange. For the joint use of data these procedures should be subject to accountability and incorporate appropriate guarantees as to the accuracy and security of the data during transmission and storage as well as procedures for recording data exchange and restrictions on the use of information exchanged.

(9) These requirements are satisfied by the Prüm Treaty. In order to meet the substantive requirements of the Hague Programme for all Member States within the time-scale set by it, the substance of the essential parts of the Prüm Treaty should become applicable to all Member States.

(10) This Decision therefore contains provisions which are based on the main provisions of the Prüm Treaty and are designed to improve the exchange of information, whereby Member States grant one another access rights to their automated DNA analysis files, automated dactyloscopic identification systems and vehicle registration data. In the case of data from national DNA analysis files and automated dactyloscopic identification systems, a hit/no hit system should enable the searching Member State, in a second step, to request specific related personal data from the Member State administering the file and, where necessary, to request further information through mutual assistance procedures, including those adopted pursuant to Framework Decision 2006/960/JHA.

(11) This would considerably speed up existing procedures enabling Member States to find out whether any other Member State, and if so, which, has the information it needs.

(12) Cross-border data comparison should open up a new dimension in crime fighting. The information obtained by comparing data should open up new investigative approaches for Member States and thus play a crucial role in assisting Member States' law enforcement and judicial authorities.

(13) The rules are based on networking Member States' national databases.

(14) Subject to certain conditions, Member States should be able to supply personal and non-personal data in order to improve the exchange of information with a view to preventing criminal offences and maintaining public order and security in connection with major events with a cross-border dimension.

(15) In the implementation of Article 12, Member States may decide to give priority to combating serious crime bearing in mind the limited technical capacities available for transmitting data.

(16) In addition to improving the exchange of information, there is a need to regulate other forms of closer cooperation between police authorities, in particular by means of joint security operations (e.g. joint patrols).

(17) Closer police and judicial cooperation in criminal matters must go hand in hand with respect for fundamental rights, in particular the right to respect for privacy and to protection of personal data, to be guaranteed by special data protection arrangements, which should be tailored to the specific nature of different forms of data exchange. Such data protection provisions should take particular account of the specific nature of cross-border online access to databases. Since, with online access, it is not possible for the Member State administering the file to make any prior checks, a system ensuring post hoc monitoring should be in place.

(18) The hit/no hit system provides for a structure of comparing anonymous profiles, where additional personal data is exchanged only after a hit, the supply and receipt of which is governed by national law, including the legal assistance rules. This set-up guarantees an adequate system of data protection, it being understood that the supply of personal data to another Member State requires an adequate level of data protection on the part of the receiving Member States.

(19) Aware of the comprehensive exchange of information and data resulting from closer police and judicial cooperation, this Decision seeks to warrant an appropriate level of data protection. It observes the level of protection designed for the processing of personal data in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Additional Protocol of 8 November 2001 to the Convention and the principles of Recommendation No R (87) 15 of the Council of Europe Regulating the Use of Personal Data in the Police Sector.

(20) The data protection provisions contained in this Decision also include data protection principles which were necessary due to the lack of a Framework Decision on data protection in the Third Pillar. This Framework Decision should be applied to the entire area of police and judicial cooperation in criminal matters under the condition that its level of data protection is not lower than the protection laid down in the Council of Europe Convention for the Protection of Individuals with regard to automatic Processing of Personal Data of 28 January 1981 and its additional Protocol of 8 November 2001 and takes account of Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, also where data are not processed automatically.

(21) Since the objectives of this Decision, in particular the improvement of information exchange in the European Union, cannot be sufficiently achieved by the Member States in isolation owing to the cross-border nature of crime fighting and security issues so that the Member States are obliged to rely on one another in these matters, and can therefore be better achieved at European Union level, the Council may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty establishing the European Community, to which Article 2 of the Treaty on European Union refers. In accordance with the principle of proportionality pursuant to Article 5 of the EC Treaty, this Decision does not go beyond what is necessary to achieve those objectives.

(22) This Decision respects the fundamental rights and observes the principles set out in particular in the Charter of Fundamental Rights of the European Union,

HAS DECIDED AS FOLLOWS:

CHAPTER 1

GENERAL ASPECTS

Article 1

Aim and scope

By means of this Decision, the Member States intend to step up cross-border cooperation in matters covered by Title VI of the Treaty, particularly the exchange of information between authorities responsible for the prevention and investigation of criminal offences. To this end, this Decision contains rules in the following areas:

(a) provisions on the conditions and procedure for the automated transfer of DNA profiles, dactyloscopic data and certain national vehicle registration data (Chapter 2);

(b) provisions on the conditions for the supply of data in connection with major events with a cross-border dimension (Chapter 3);

(c) provisions on the conditions for the supply of information in order to prevent terrorist offences (Chapter 4);

(d) provisions on the conditions and procedure for stepping up cross-border police cooperation through various measures (Chapter 5).

CHAPTER 2

ONLINE ACCESS AND FOLLOW-UP REQUESTS

SECTION 1

DNA profiles

Article 2

Establishment of national DNA analysis files

1. Member States shall open and keep national DNA analysis files for the investigation of criminal offences. Processing of data kept in those files, under this Decision, shall be carried out in accordance with this Decision, in compliance with the national law applicable to the processing.

2. For the purpose of implementing this Decision, the Member States shall ensure the availability of reference data from their national DNA analysis files as referred to in the first sentence of paragraph 1. Reference data shall only include DNA profiles established from the non-coding part of DNA and a reference number. Reference data shall not contain any data from which the data subject can be directly identified. Reference data which is not attributed to any individual (unidentified DNA profiles) shall be recognisable as such.

3. Each Member State shall inform the General Secretariat of the Council of the national DNA analysis files to which Articles 2 to 6 apply and the conditions for automated searching as referred to in Article 3(1) in accordance with Article 36.

Article 3

Automated searching of DNA profiles

1. For the investigation of criminal offences, Member States shall allow other Member States' national contact points as referred to in Article 6, access to the reference data in their DNA analysis files, with the power to conduct automated searches by comparing DNA profiles. Searches may be conducted only in individual cases and in compliance with the requesting Member State's national law.

2. Should an automated search show that a DNA profile supplied matches DNA profiles entered in the receiving Member State's searched file, the national contact point of the searching Member State shall receive in an automated way the reference data with which a match has been found. If no match can be found, automated notification of this shall be given.

Article 4

Automated comparison of DNA profiles

1. For the investigation of criminal offences, the Member States shall, by mutual consent, via their national contact points, compare the DNA profiles of their unidentified DNA profiles with all DNA profiles from other national DNA analysis files' reference data. Profiles shall be supplied and compared in automated form. Unidentified DNA profiles shall be supplied for comparison only where provided for under the requesting Member State's national law.

2. Should a Member State, as a result of the comparison referred to in paragraph 1, find that any DNA profiles supplied match any of those in its DNA analysis files, it shall, without delay, supply the other Member State's national contact point with the reference data with which a match has been found.

Article 5

Supply of further personal data and other information

Should the procedures referred to in Articles 3 and 4 show a match between DNA profiles, the supply of further available personal data and other information relating to the reference data shall be governed by the national law, including the legal assistance rules, of the requested Member State.

Article 6

National contact point and implementing measures

1. For the purposes of the supply of data as referred to in Articles 3 and 4, each Member State shall designate a national contact point. The powers of the national contact points shall be governed by the applicable national law.

2. Details of technical arrangements for the procedures set out in Articles 3 and 4 shall be laid down in the implementing measures as referred to in Article 33.

Article 7

Collection of cellular material and supply of DNA profiles

Where, in ongoing investigations or criminal proceedings, there is no DNA profile available for a particular individual present within a requested Member State's territory, the requested Member State shall provide legal assistance by collecting and examining cellular material from that individual and by supplying the DNA profile obtained, if:

(a) the requesting Member State specifies the purpose for which this is required;

(b) the requesting Member State produces an investigation warrant or statement issued by the competent authority, as required under that Member State's law, showing that the requirements for collecting and examining cellular material would be fulfilled if the individual concerned were present within the requesting Member State's territory; and

(c) under the requested Member State's law, the requirements for collecting and examining cellular material and for supplying the DNA profile obtained are fulfilled.

SECTION 2

Dactyloscopic data

Article 8

Dactyloscopic data

For the purpose of implementing this Decision, Member States shall ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offences. Reference data shall only include dactyloscopic data and a reference number. Reference data shall not contain any data from which the data subject can be directly identified. Reference data which is not attributed to any individual (unidentified dactyloscopic data) must be recognisable as such.

Article 9

Automated searching of dactyloscopic data

1. For the prevention and investigation of criminal offences, Member States shall allow other Member States' national contact points, as referred to in Article 11, access to the reference data in the automated fingerprint identification systems which they have established for that purpose, with the power to conduct automated searches by comparing dactyloscopic data. Searches may be conducted only in individual cases and in compliance with the requesting Member State's national law.

2. The confirmation of a match of dactyloscopic data with reference data held by the Member State administering the file shall be carried out by the national contact point of the requesting Member State by means of the automated supply of the reference data required for a clear match.

Article 10

Supply of further personal data and other information

Should the procedure referred to in Article 9 show a match between dactyloscopic data, the supply of further available personal data and other information relating to the reference data shall be governed by the national law, including the legal assistance rules, of the requested Member State.

Article 11

National contact point and implementing measures

1. For the purposes of the supply of data as referred to in Article 9, each Member State shall designate a national contact point. The powers of the national contact points shall be governed by the applicable national law.

2. Details of technical arrangements for the procedure set out in Article 9 shall be laid down in the implementing measures as referred to in Article 33.

SECTION 3

Vehicle registration data

Article 12

Automated searching of vehicle registration data

1. For the prevention and investigation of criminal offences and in dealing with other offences coming within the jurisdiction of the courts or the public prosecution service in the searching Member State, as well as in maintaining public security, Member States shall allow other Member States' national contact points, as referred to in paragraph 2, access to the following national vehicle registration data, with the power to conduct automated searches in individual cases:

(a) data relating to owners or operators; and

(b) data relating to vehicles.

Searches may be conducted only with a full chassis number or a full registration number. Searches may be conducted only in compliance with the searching Member State's national law.

2. For the purposes of the supply of data as referred to in paragraph 1, each Member State shall designate a national contact point for incoming requests. The powers of the national contact points shall be governed by the applicable national law. Details of technical arrangements for the procedure shall be laid down in the implementing measures as referred to in Article 33.

CHAPTER 3

MAJOR EVENTS

Article 13

Supply of non-personal data

For the prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension, in particular for sporting events or European Council meetings, Member States shall, both upon request and of their own accord, in compliance with the supplying Member State's national law, supply one another with any non-personal data required for those purposes.

Article 14

Supply of personal data

1. For the prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension, in particular for sporting events or European Council meetings, Member States shall, both upon request and of their own accord, supply one another with personal data if any final convictions or other circumstances give reason to believe that the data subjects will commit criminal offences at the events or pose a threat to public order and security, in so far as the supply of such data is permitted under the supplying Member State's national law.

2. Personal data may be processed only for the purposes laid down in paragraph 1 and for the specified events for which they were supplied. The data supplied must be deleted without delay once the purposes referred to in paragraph 1 have been achieved or can no longer be achieved. The data supplied must in any event be deleted after not more than a year.

Article 15

National contact point

For the purposes of the supply of data as referred to in Articles 13 and 14, each Member State shall designate a national contact point. The powers of the national contact points shall be governed by the applicable national law.

CHAPTER 4

MEASURES TO PREVENT TERRORIST OFFENCES

Article 16

Supply of information in order to prevent terrorist offences

1. For the prevention of terrorist offences, Member States may, in compliance with national law, in individual cases, even without being requested to do so, supply other Member States' national contact points, as referred to in paragraph 3, with the personal data and information specified in paragraph 2, in so far as is necessary because particular circumstances give reason to believe that the data subjects will commit criminal offences as referred to in Articles 1 to 3 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism ([1]).

([1]) OJ L 164, 22.6.2002, p. 3.

2. The data to be supplied shall comprise surname, first names, date and place of birth and a description of the circumstances giving rise to the belief referred to in paragraph 1.

3. Each Member State shall designate a national contact point for exchange of information with other Member States' national contact points. The powers of the national contact points shall be governed by the applicable national law.

4. The supplying Member State may, in compliance with national law, impose conditions on the use made of such data and information by the receiving Member State. The receiving Member State shall be bound by any such conditions.

CHAPTER 5

OTHER FORMS OF COOPERATION

Article 17

Joint operations

1. In order to step up police cooperation, the competent authorities designated by the Member States may, in maintaining public order and security and preventing criminal offences, introduce joint patrols and other joint operations in which designated officers or other officials (officers) from other Member States participate in operations within a Member State's territory.

2. Each Member State may, as a host Member State, in compliance with its own national law, and with the seconding Member State's consent, confer executive powers on the seconding Member States' officers involved in joint operations or, in so far as the host Member State's law permits, allow the seconding Member States' officers to exercise their executive powers in accordance with the seconding Member State's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of officers from the host Member State. The seconding Member States' officers shall be subject to the host Member State's national law. The host Member State shall assume responsibility for their actions.

3. Seconding Member States' officers involved in joint operations shall be subject to the instructions given by the host Member State's competent authority.

4. Member States shall submit declarations as referred to in Article 36 in which they lay down the practical aspects of cooperation.

Article 18

Assistance in connection with mass gatherings disasters and serious accidents

Member States' competent authorities shall provide one another with mutual assistance, in compliance with national law, in connection with mass gatherings and similar major events, disasters and serious accidents, by seeking to prevent criminal offences and maintain public order and security by:

(a) notifying one another as promptly as possible of such situations with a cross-border impact and exchanging any relevant information;

(b) taking and coordinating the necessary policing measures within their territory in situations with a cross-border impact;

(c) as far as possible, dispatching officers, specialists and advisers and supplying equipment, at the request of the Member State within whose territory the situation has arisen.

Article 19

Use of arms, ammunition and equipment

1. Officers from a seconding Member State who are involved in a joint operation within another Member State's territory pursuant to Article 17 or 18 may wear their own national uniforms there. They may carry such arms, ammunition and equipment as they are allowed to under the seconding Member State's national law. The host Member State may prohibit the carrying of particular arms, ammunition or equipment by a seconding Member State's officers.

2. Member States shall submit declarations as referred to in Article 36 in which they list the arms, ammunition and equipment that may be used only in legitimate self-defence or in the defence of others. The host Member State's officer in actual charge of the operation may in individual cases, in compliance with national law, give permission for arms, ammunition and equipment to be used for purposes going beyond those specified in the first sentence. The use of arms, ammunition and equipment shall be governed by the host Member State's law. The competent authorities shall inform one another of the arms, ammunition and equipment permitted and of the conditions for their use.

3. If officers from a Member State make use of vehicles in action under this Decision within another Member State's territory, they shall be subject to the same road traffic regulations as the host Member State's officers, including as regards right of way and any special privileges.

4. Member States shall submit declarations as referred to in Article 36 in which they lay down the practical aspects of the use of arms, ammunition and equipment.

Article 20

Protection and assistance

Member States shall be required to provide other Member States' officers crossing borders with the same protection and assistance in the course of those officers' duties as for their own officers.

Article 21

General rules on civil liability

1. Where officials of a Member State are operating in another Member State pursuant to Article 17, their Member State shall be liable for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

2. The Member State in whose territory the damage referred to in paragraph 1 was caused shall make good such damage under the conditions applicable to damage caused by its own officials.

3. In the case provided for in paragraph 1, the Member State whose officials have caused damage to any person in the territory of another Member State shall reimburse the latter in full any sums it has paid to the victims or persons entitled on their behalf.

4. Where officials of a Member State are operating in another Member State pursuant to Article 18, the latter Member State shall be liable in accordance with its national law for any damage caused by them during their operations.

5. Where the damage referred to in paragraph 4 results from gross negligence or wilful misconduct, the host Member State may approach the seconding Member State in order to have any sums it has paid to the victims or persons entitled on their behalf reimbursed by the latter.

6. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 3, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement of damages it has sustained from another Member State.

Article 22

Criminal liability

Officers operating within another Member State's territory under this Decision, shall be treated in the same way as officers of the host Member State with regard to any criminal offences that might be committed by, or against them, save as otherwise provided in another agreement which is binding on the Member States concerned.

Article 23

Employment relationship

Officers operating within another Member State's territory, under this Decision, shall remain subject to the employment law provisions applicable in their own Member State, particularly as regards disciplinary rules.

CHAPTER 6

GENERAL PROVISIONS ON DATA PROTECTION

Article 24

Definitions and scope

1. For the purposes of this Decision:

(a) 'processing of personal data' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of data. Processing within the meaning of this Decision shall also include notification of whether or not a hit exists;

(b) 'automated search procedure' shall mean direct access to the automated files of another body where the response to the search procedure is fully automated;

(c) 'referencing' shall mean the marking of stored personal data without the aim of limiting their processing in future;

(d) 'blocking' shall mean the marking of stored personal data with the aim of limiting their processing in future.

2. The following provisions shall apply to data which are or have been supplied pursuant to this Decision, save as otherwise provided in the preceding Chapters.

Article 25

Level of data protection

1. As regards the processing of personal data which are or have been supplied pursuant to this Decision, each Member State shall guarantee a level of protection of personal data in its national law at least equal to that resulting from the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and its Additional Protocol of 8 November 2001 and in doing so, shall take account of Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe to the Member States regulating the use of personal data in the police sector, also where data are not processed automatically.

2. The supply of personal data provided for under this Decision may not take place until the provisions of this Chapter have been implemented in the national law of the territories of the Member States involved in such supply. The Council shall unanimously decide whether this condition has been met.

3. Paragraph 2 shall not apply to those Member States where the supply of personal data as provided for in this Decision has already started pursuant to the Treaty of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration (Prüm Treaty).

Article 26

Purpose

1. Processing of personal data by the receiving Member State shall be permitted solely for the purposes for which the data have been supplied in accordance with this Decision. Processing for other purposes shall be permitted solely with the prior authorisation of the Member State administering the file and subject only to the national law of the receiving Member State. Such authorisation may be granted provided that processing for such other purposes is permitted under the national law of the Member State administering the file.

2. Processing of data supplied pursuant to Articles 3, 4 and 9 by the searching or comparing Member State shall be permitted solely in order to:

(a) establish whether the compared DNA profiles or dactyloscopic data match;

(b) prepare and submit a police or judicial request for legal assistance in compliance with national law if those data match;

(c) record within the meaning of Article 30.

The Member State administering the file may process the data supplied to it in accordance with Articles 3, 4 and 9 solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording pursuant to Article 30. The supplied data shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned under points (b) and (c) of the first subparagraph.

3. Data supplied in accordance with Article 12 may be used by the Member State administering the file solely where this is necessary for the purpose of providing automated replies to search procedures or recording as specified in Article 30. The data supplied shall be deleted immediately following automated replies to searches unless further processing is necessary for recording pursuant to Article 30. The searching Member State may use data received in a reply solely for the procedure for which the search was made.

Article 27

Competent authorities

Personal data supplied may be processed only by the authorities, bodies and courts with responsibility for a task in furtherance of the aims mentioned in Article 26. In particular, data may be supplied to other entities only with the prior authorisation of the supplying Member State and in compliance with the law of the receiving Member State.

Article 28

Accuracy, current relevance and storage time of data

1. The Member States shall ensure the accuracy and current relevance of personal data. Should it transpire *ex officio* or from a notification by the data subject, that incorrect data or data which should not have been supplied have been supplied, this shall be notified without delay to the receiving Member State or Member States. The Member State or Member States concerned shall be obliged to correct or delete the data. Moreover, personal data supplied shall be corrected if they are found to be incorrect. If the receiving body has reason to believe that the supplied data are incorrect or should be deleted the supplying body shall be informed forthwith.

2. Data, the accuracy of which the data subject contests and the accuracy or inaccuracy of which cannot be established shall, in accordance with the national law of the Member States, be marked with a flag at the request of the data subject. If a flag exists, this may be removed subject to the national law of the Member States and only with the permission of the data subject or based on a decision of the competent court or independent data protection authority.

3. Personal data supplied which should not have been supplied or received shall be deleted. Data which are lawfully supplied and received shall be deleted:

(a) if they are not or no longer necessary for the purpose for which they were supplied; if personal data have been supplied without request, the receiving body shall immediately check if they are necessary for the purposes for which they were supplied;

(b) following the expiry of the maximum period for keeping data laid down in the national law of the supplying Member State where the supplying body informed the receiving body of that maximum period at the time of supplying the data.

Where there is reason to believe that deletion would prejudice the interests of the data subject, the data shall be blocked instead of being deleted in compliance with national law. Blocked data may be supplied or used solely for the purpose which prevented their deletion.

Article 29

Technical and organisational measures to ensure data protection and data security

1. The supplying and receiving bodies shall take steps to ensure that personal data is effectively protected against accidental or unauthorised destruction, accidental loss, unauthorised access, unauthorised or accidental alteration and unauthorised disclosure.

2. The features of the technical specification of the automated search procedure are regulated in the implementing measures as referred to in Article 33 which guarantee that:

(a) state-of-the-art technical measures are taken to ensure data protection and data security, in particular data confidentiality and integrity;

(b) encryption and authorisation procedures recognised by the competent authorities are used when having recourse to generally accessible networks; and

(c) the admissibility of searches in accordance with Article 30(2), (4) and (5) can be checked.

Article 30

Logging and recording: special rules governing automated and non-automated supply

1. Each Member State shall guarantee that every non-automated supply and every non-automated receipt of personal data by the body administering the file and by the searching body is logged in order to verify the admissibility of the supply. Logging shall contain the following information:

(a) the reason for the supply;

(b) the data supplied;

(c) the date of the supply; and

(d) the name or reference code of the searching body and of the body administering the file.

2. The following shall apply to automated searches for data based on Articles 3, 9 and 12 and to automated comparison pursuant to Article 4:

(a) only specially authorised officers of the national contact points may carry out automated searches or comparisons. The list of officers authorised to carry out automated searches or comparisons shall be made available upon request to the supervisory authorities referred to in paragraph 5 and to the other Member States;

(b) each Member State shall ensure that each supply and receipt of personal data by the body administering the file and the searching body is recorded, including notification of whether or not a hit exists. Recording shall include the following information:

(i) the data supplied;

(ii) the date and exact time of the supply; and

(iii) the name or reference code of the searching body and of the body administering the file.

The searching body shall also record the reason for the search or supply as well as an identifier for the official who carried out the search and the official who ordered the search or supply.

3. The recording body shall immediately communicate the recorded data upon request to the competent data protection authorities of the relevant Member State at the latest within four weeks following receipt of the request. Recorded data may be used solely for the following purposes:

(a) monitoring data protection;

(b) ensuring data security.

4. The recorded data shall be protected with suitable measures against inappropriate use and other forms of improper use and shall be kept for two years. After the conservation period the recorded data shall be deleted immediately.

5. Responsibility for legal checks on the supply or receipt of personal data lies with the independent data protection authorities or, as appropriate, the judicial authorities of the respective Member States. Anyone can request these authorities to check the lawfulness of the processing of data in respect of their person in compliance with national law. Independently of such requests, these authorities and the bodies responsible for recording shall carry out random checks on the lawfulness of supply, based on the files involved.

The results of such checks shall be kept for inspection for 18 months by the independent data protection authorities. After this period, they shall be immediately deleted. Each data protection authority may be requested by the independent data protection authority of another Member State to exercise its powers in accordance with national law. The independent data protection authorities of the Member States shall perform the inspection tasks necessary for mutual cooperation, in particular by exchanging relevant information.

Article 31

Data subjects' rights to information and damages

1. At the request of the data subject under national law, information shall be supplied in compliance with national law to the data subject upon production of proof of his identity, without unreasonable expense, in general comprehensible terms and without unacceptable delays, on the data processed in respect of his person, the origin of the data, the recipient or groups of recipients, the intended purpose of the processing and, where required by national law, the legal basis for the processing. Moreover, the data subject shall be entitled to have inaccurate data corrected and unlawfully processed data deleted. The Member States shall also ensure that, in the event of violation of his rights in relation to data protection, the data subject shall be able to lodge an effective complaint to an independent court or a tribunal within the meaning of Article 6(1) of the European Convention on Human Rights or an independent supervisory authority within the meaning of Article 28 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1] and that he is given the possibility to claim for damages or to seek another form of legal compensation. The detailed rules for the procedure to assert these rights and the reasons for limiting the right of access shall be governed by the relevant national legal provisions of the Member State where the data subject asserts his rights.

2. Where a body of one Member State has supplied personal data under this Decision, the receiving body of the other Member State cannot use the inaccuracy of the data supplied as grounds to evade its liability vis-à-vis the injured party under national law. If damages are awarded against the receiving body because of its use of inaccurate transfer data, the body which supplied the data shall refund the amount paid in damages to the receiving body in full.

Article 32

Information requested by the Member States

The receiving Member State shall inform the supplying Member State on request of the processing of supplied data and the result obtained.

CHAPTER 7

IMPLEMENTING AND FINAL PROVISIONS

Article 33

Implementing measures

The Council, acting by a qualified majority and after Consulting the European Parliament, shall adopt measures necessary to implement this Decision at the level of the Union.

[1] OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

Article 34

Costs

Each Member State shall bear the operational costs incurred by its own authorities in connection with the application of this Decision. In special cases, the Member States concerned may agree on different arrangements.

Article 35

Relationship with other instruments

1. For the Member States concerned, the relevant provisions of this Decision shall be applied instead of the corresponding provisions contained in the Prüm Treaty. Any other provision of the Prüm Treaty shall remain applicable between the contracting parties of the Prüm Treaty.

2. Without prejudice to their commitments under other acts adopted pursuant to Title VI of the Treaty:

(a) Member States may continue to apply bilateral or multilateral agreements or arrangements on cross-border cooperation which are in force on the date this Decision is adopted in so far as such agreements or arrangements are not incompatible with the objectives of this Decision;

(b) Member States may conclude or bring into force bilateral or multilateral agreements or arrangements on cross-border cooperation after this Decision has entered into force in so far as such agreements or arrangements provide for the objectives of this Decision to be extended or enlarged.

3. The agreements and arrangements referred to in paragraphs 1 and 2 may not affect relations with Member States which are not parties thereto.

4. Within four weeks of this Decision taking effect Member States shall inform the Council and the Commission of existing agreements or arrangements within the meaning of paragraph 2(a) which they wish to continue to apply.

5. Member States shall also inform the Council and the Commission of all new agreements or arrangements within the meaning of paragraph 2(b) within three months of their signing or, in the case of instruments which were signed before adoption of this Decision, within three months of their entry into force.

6. Nothing in this Decision shall affect bilateral or multilateral agreements or arrangements between Member States and third States.

7. This Decision shall be without prejudice to existing agreements on legal assistance or mutual recognition of court decisions.

Article 36

Implementation and declarations

1. Member States shall take the necessary measures to comply with the provisions of this Decision within one year of this Decision taking effect, with the exception of the provisions of Chapter 2 with respect to which the necessary measures shall be taken within three years of this Decision and the Council Decision on the implementation of this Decision taking effect.

2. Member States shall inform the General Secretariat of the Council and the Commission that they have implemented the obligations imposed on them under this Decision and submit the declarations foreseen by this Decision. When doing so, each Member State may indicate that it will apply immediately this Decision in its relations with those Member States which have given the same notification.

3. Declarations submitted in accordance with paragraph 2 may be amended at any time by means of a declaration submitted to the General Secretariat of the Council. The General Secretariat of the Council shall forward any declarations received to the Member States and the Commission.

4. On the basis of this and other information made available by Member States on request, the Commission shall submit a report to the Council by 28 July 2012 on the implementation of this Decision accompanied by such proposals as it deems appropriate for any further development.

Article 37

Application

This Decision shall take effect 20 days following its publication in the *Official Journal of the European Union*.

Done at Luxembourg, 23 June 2008.

For the Council

The President

I. JARC

COUNCIL DECISION 2008/616/JHA

of 23 June 2008

on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to Article 33 of Council Decision 2008/615/JHA [1],

Having regard to the initiative of the Federal Republic of Germany,

Having regard to the opinion of the European Parliament [2],

Whereas:

(1) On 23 June 2008 the Council adopted Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

(2) By means of Decision 2008/615/JHA, the basic elements of the Treaty of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration (hereinafter the Prüm Treaty), were transposed into the legal framework of the European Union.

(3) Article 33 of Decision 2008/615/JHA provides that the Council is to adopt the measures necessary to implement Decision 2008/615/JHA at the level of the Union in accordance with the procedure laid down in the second sentence of Article 34(2)(c) of the Treaty on European Union. These measures are to be based on the Implementing Agreement of 5 December 2006 concerning the administrative and technical implementation and application of the Prüm Treaty.

(4) This Decision establishes those common normative provisions which are indispensable for administrative and technical implementation of the forms of cooperation set out in Decision 2008/615/JHA. The Annex to this Decision contains implementing provisions of a technical nature. In addition, a separate Manual, containing exclusively factual information to be provided by the Member States, will be drawn up and kept up to date by the General Secretariat of the Council.

(5) Having regard to technical capabilities, routine searches of new DNA profiles will in principle be carried out by means of single searches, and appropriate solutions for this will be found at the technical level,

HAS DECIDED AS FOLLOWS:

CHAPTER I

GENERAL

Article 1

Aim

The aim of this Decision is to lay down the necessary administrative and technical provisions for the implementation of Decision 2008/615/JHA, in particular as regards the automated exchange of DNA data, dactyloscopic data and vehicle registration data, as set out in Chapter 2 of that Decision, and other forms of cooperation, as set out in Chapter 5 of that Decision.

Article 2

Definitions

For the purposes of this Decision:

(a) 'search' and 'comparison', as referred to in Articles 3, 4 and 9 of Decision 2008/615/JHA, mean the procedures by which it is established whether there is a match between, respectively, DNA data or dactyloscopic data which have been communicated by one Member State and DNA data or dactyloscopic data stored in the databases of one, several, or all of the Member States;

(b) 'automated searching', as referred to in Article 12 of Decision 2008/615/JHA, means an online access procedure for consulting the databases of one, several, or all of the Member States;

(c) 'DNA profile' means a letter or number code which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample, i.e. the particular molecular structure at the various DNA locations (loci);

(d) 'non-coding part of DNA' means chromosome regions not genetically expressed, i.e. not known to provide for any functional properties of an organism;

[1] See page 1 of this Official Journal.
[2] Opinion of 21 April 2008 (not yet published in the Official Journal).

(e) 'DNA reference data' mean DNA profile and reference number;

(f) 'reference DNA profile' means the DNA profile of an identified person;

(g) 'unidentified DNA profile' means the DNA profile obtained from traces collected during the investigation of criminal offences and belonging to a person not yet identified;

(h) 'note' means a Member State's marking on a DNA profile in its national database indicating that there has already been a match for that DNA profile on another Member State's search or comparison;

(i) 'dactyloscopic data' mean fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae), when they are stored and dealt with in an automated database;

(j) 'vehicle registration data' mean the data-set as specified in Chapter 3 of the Annex to this Decision;

(k) 'individual case', as referred to in Article 3(1), second sentence, Article 9(1), second sentence and Article 12(1) of Decision 2008/615/JHA, means a single investigation or prosecution file. If such a file contains more than one DNA profile, or one piece of dactyloscopic data or vehicle registration data, they may be transmitted together as one request.

CHAPTER 2

COMMON PROVISIONS FOR DATA EXCHANGE

Article 3

Technical specifications

Member States shall observe common technical specifications in connection with all requests and answers related to searches and comparisons of DNA profiles, dactyloscopic data and vehicle registration data. These technical specifications are laid down in the Annex to this Decision.

Article 4

Communications network

The electronic exchange of DNA data, dactyloscopic data and vehicle registration data between Member States shall take place using the Trans European Services for Telematics between Administrations (TESTA II) communications network and further developments thereof.

Article 5

Availability of automated data exchange

Member States shall take all necessary measures to ensure that automated searching or comparison of DNA data, dactyloscopic data and vehicle registration data is possible 24 hours a day and seven days a week. In the event of a technical fault, the Member States' national contact points shall immediately inform each other and shall agree on temporary alternative information exchange arrangements in accordance with the legal provisions applicable. Automated data exchange shall be re-established as quickly as possible.

Article 6

Reference numbers for DNA data and dactyloscopic data

The reference numbers referred to in Article 2 and Article 8 of Decision 2008/615/JHA shall consist of a combination of the following:

(a) a code allowing the Member States, in the case of a match, to retrieve personal data and other information in their databases in order to supply it to one, several or all of the Member States in accordance with Article 5 or Article 10 of Decision 2008/615/JHA;

(b) a code to indicate the national origin of the DNA profile or dactyloscopic data; and

(c) with respect to DNA data, a code to indicate the type of DNA profile.

CHAPTER 3

DNA DATA

Article 7

Principles of DNA data exchange

1. Member States shall use existing standards for DNA data exchange, such as the European Standard Set (ESS) or the Interpol Standard Set of Loci (ISSOL).

2. The transmission procedure, in the case of automated searching and comparison of DNA profiles, shall take place within a decentralised structure.

3. Appropriate measures shall be taken to ensure confidentiality and integrity for data being sent to other Member States, including their encryption.

4. Member States shall take the necessary measures to guarantee the integrity of the DNA profiles made available or sent for comparison to the other Member States and to ensure that these measures comply with international standards such as ISO 17025.

5. Member States shall use Member State codes in accordance with the ISO 3166-1 alpha-2 standard.

Article 8

Rules for requests and answers in connection with DNA data

1. A request for an automated search or comparison, as referred to in Articles 3 or 4 of Decision 2008/615/JHA, shall include only the following information:

(a) the Member State code of the requesting Member State;

(b) the date, time and indication number of the request;

(c) DNA profiles and their reference numbers;

(d) the types of DNA profiles transmitted (unidentified DNA profiles or reference DNA profiles); and

(e) information required for controlling the database systems and quality control for the automatic search processes.

2. The answer (matching report) to the request referred to in paragraph 1 shall contain only the following information:

(a) an indication as to whether there were one or more matches (hits) or no matches (no hits);

(b) the date, time and indication number of the request;

(c) the date, time and indication number of the answer;

(d) the Member State codes of the requesting and requested Member States;

(e) the reference numbers of the requesting and requested Member States;

(f) the type of DNA profiles transmitted (unidentified DNA profiles or reference DNA profiles);

(g) the requested and matching DNA profiles; and

(h) information required for controlling the database systems and quality control for the automatic search processes.

3. Automated notification of a match shall only be provided if the automated search or comparison has resulted in a match of a minimum number of loci. This minimum is set out in Chapter 1 of the Annex to this Decision.

4. The Member States shall ensure that requests comply with declarations issued pursuant to Article 2(3) of Decision 2008/615/JHA. These declarations shall be reproduced in the Manual referred to in Article 18(2) of this Decision.

Article 9

Transmission procedure for automated searching of unidentified DNA profiles in accordance with Article 3 of Decision 2008/615/JHA

1. If, in a search with an unidentified DNA profile, no match has been found in the national database or a match has been found with an unidentified DNA profile, the unidentified DNA profile may then be transmitted to all other Member States' databases and if, in a search with this unidentified DNA profile, matches are found with reference DNA profiles and/or unidentified DNA profiles in other Member States' databases, these matches shall be automatically communicated and the DNA reference data transmitted to the requesting Member State; if no matches can be found in other Member States' databases, this shall be automatically communicated to the requesting Member State.

2. If, in a search with an unidentified DNA profile, a match is found in other Member States' databases, each Member State concerned may insert a note to this effect in its national database.

Article 10

Transmission procedure for automated search of reference DNA profiles in accordance with Article 3 of Decision 2008/615/JHA

If, in a search with a reference DNA profile, no match has been found in the national database with a reference DNA profile or a match has been found with an unidentified DNA profile, this reference DNA profile may then be transmitted to all other Member States' databases and if, in a search with this reference DNA profile, matches are found with reference DNA profiles and/or unidentified DNA profiles in other Member States' databases, these matches shall be automatically communicated and the DNA reference data transmitted to the requesting Member State; if no matches can be found in other Member States' databases, it shall be automatically communicated to the requesting Member State.

Article 11

Transmission procedure for automated comparison of unidentified DNA profiles in accordance with Article 4 of Decision 2008/615/JHA

1. If, in a comparison with unidentified DNA profiles, matches are found in other Member States' databases with reference DNA profiles and/or unidentified DNA profiles, these matches shall be automatically communicated and the DNA reference data transmitted to the requesting Member State.

2. If, in a comparison with unidentified DNA profiles, matches are found in other Member States' databases with unidentified DNA profiles or reference DNA profiles, each Member State concerned may insert a note to this effect in its national database.

CHAPTER 4

DACTYLOSCOPIC DATA

Article 12

Principles for the exchange of dactyloscopic data

1. The digitalisation of dactyloscopic data and their transmission to the other Member States shall be carried out in accordance with the uniform data format specified in Chapter 2 of the Annex to this Decision.

2. Each Member State shall ensure that the dactyloscopic data it transmits are of sufficient quality for a comparison by the automated fingerprint identification systems (AFIS).

3. The transmission procedure for the exchange of dactyloscopic data shall take place within a decentralised structure.

4. Appropriate measures shall be taken to ensure the confidentiality and integrity of dactyloscopic data being sent to other Member States, including their encryption.

5. The Member States shall use Member State codes in accordance with the ISO 3166-1 alpha-2 standard.

Article 13

Search capacities for dactyloscopic data

1. Each Member State shall ensure that its search requests do not exceed the search capacities specified by the requested Member State. Member States shall submit declarations as referred to in Article 18(2) to the General Secretariat of the Council in which they lay down their maximum search capacities per day for dactyloscopic data of identified persons and for dactyloscopic data of persons not yet identified.

2. The maximum numbers of candidates accepted for verification per transmission are set out in Chapter 2 of the Annex to this Decision.

Article 14

Rules for requests and answers in connection with dactyloscopic data

1. The requested Member State shall check the quality of the transmitted dactyloscopic data without delay by a fully automated procedure. Should the data be unsuitable for an automated comparison, the requested Member State shall inform the requesting Member State without delay.

2. The requested Member State shall conduct searches in the order in which requests are received. Requests shall be processed within 24 hours by a fully automated procedure. The requesting Member State may, if its national law so prescribes, ask for accelerated processing of its requests and the requested Member State shall conduct these searches without delay. If deadlines cannot be met for reasons of *force majeure*, the comparison shall be carried out without delay as soon as the impediments have been removed.

CHAPTER 5

VEHICLE REGISTRATION DATA

Article 15

Principles of automated searching of vehicle registration data

1. For automated searching of vehicle registration data Member States shall use a version of the European Vehicle and Driving Licence Information System (Eucaris) software application especially designed for the purposes of Article 12 of Decision 2008/615/JHA, and amended versions of this software.

2. Automated searching of vehicle registration data shall take place within a decentralised structure.

3. The information exchanged via the Eucaris system shall be transmitted in encrypted form.

4. The data elements of the vehicle registration data to be exchanged are specified in Chapter 3 of the Annex to this Decision.

5. In the implementation of Article 12 of Decision 2008/615/JHA, Member States may give priority to searches related to combating serious crime.

Article 16

Costs

Each Member State shall bear the costs arising from the administration, use and maintenance of the Eucaris software application referred to in Article 15(1).

CHAPTER 6

POLICE COOPERATION

Article 17

Joint patrols and other joint operations

1. In accordance with Chapter 5 of Decision 2008/615/JHA, and in particular with the declarations submitted pursuant to Articles 17(4), 19(2), and 19(4) of that Decision, each Member State shall designate one or more contact points in order to allow

other Member States to address competent authorities and each Member State may specify its procedures for setting up joint patrols and other joint operations, its procedures for initiatives from other Member States with regard to those operations, as well as other practical aspects, and operational modalities in relation to those operations.

2. The General Secretariat of the Council shall compile and keep up to date a list of the contact points and shall inform the competent authorities about any change to that list.

3. The competent authorities of each Member State may take the initiative to set up a joint operation. Before the start of a specific operation, the competent authorities referred to in paragraph 2 shall make written or verbal arrangements that may cover details such as:

(a) the competent authorities of the Member States for the operation;

(b) the specific purpose of the operation;

(c) the host Member State where the operation is to take place;

(d) the geographical area of the host Member State where the operation is to take place;

(e) the period covered by the operation;

(f) the specific assistance to be provided by the seconding Member State(s) to the host Member State, including officers or other officials, material and financial elements;

(g) the officers participating in the operation;

(h) the officer in charge of the operation;

(i) the powers that the officers and other officials of the seconding Member State(s) may exercise in the host Member State during the operation;

(j) the particular arms, ammunition and equipment that the seconding officers may use during the operation in accordance with Decision 2008/615/JHA;

(k) the logistic modalities as regards transport, accommodation and security;

(l) the allocation of the costs of the joint operation if it differs from that provided in the first sentence of Article 34 of Decision 2008/615/JHA;

(m) any other possible elements required.

4. The declarations, procedures and designations provided for in this Article shall be reproduced in the Manual referred to in Article 18(2).

CHAPTER 7

FINAL PROVISIONS

Article 18

Annex and Manual

1. Further details concerning the technical and administrative implementation of Decision 2008/615/JHA are set out in the Annex to this Decision.

2. A Manual shall be prepared and kept up to date by the General Secretariat of the Council, comprising exclusively factual information provided by the Member States through declarations made pursuant to Decision 2008/615/JHA or this Decision or through notifications made to the General Secretariat of the Council. The Manual shall be in the form of a Council Document.

Article 19

Independent data protection authorities

Member States shall, in accordance with Article 18(2) of this Decision, inform the General Secretariat of the Council of the independent data protection authorities or the judicial authorities as referred to in Article 30(5) of Decision 2008/615/JHA.

Article 20

Preparation of decisions as referred to in Article 25(2) of Decision 2008/615/JHA

1. The Council shall take a decision as referred to in Article 25(2) of Decision 2008/615/JHA on the basis of an evaluation report which shall be based on a questionnaire.

2. With respect to the automated data exchange in accordance with Chapter 2 of Decision 2008/615/JHA, the evaluation report shall also be based on an evaluation visit and a pilot run that shall be carried out when the Member State concerned has informed the General Secretariat in accordance with the first sentence of Article 36(2) of Decision 2008/615/JHA.

3. Further details of the procedure are set out in Chapter 4 of the Annex to this Decision.

Article 21

Evaluation of the data exchange

1. An evaluation of the administrative, technical and financial application of the data exchange pursuant to Chapter 2 of Decision 2008/615/JHA, and in particular the use of the mechanism of Article 15(5), shall be carried out on a regular basis. The evaluation shall relate to those Member States already applying Decision 2008/615/JHA at the time of the evaluation and shall be carried out with respect to the data categories for

which data exchange has started among the Member States concerned. The evaluation shall be based on reports of the respective Member States.

2. Further details of the procedure are set out in Chapter 4 of the Annex to this Decision.

Article 22

Relationship with the Implementing Agreement of the Prüm Treaty

For the Member States bound by the Prüm Treaty, the relevant provisions of this Decision and the Annex hereto once fully implemented shall apply instead of the corresponding provisions contained in the Implementing Agreement of the Prüm Treaty. Any other provisions of the Implementing Agreement shall remain applicable between the contracting parties of the Prüm Treaty.

Article 23

Implementation

Member States shall take the necessary measures to comply with the provisions of this Decision within the periods referred to in Article 36(1) of Decision 2008/615/JHA.

Article 24

Application

This Decision shall take effect 20 days following its publication in the *Official Journal of the European Union*.

Done at Luxembourg, 23 June 2008.

For the Council

The President

I. JARC

ANNEX

TABLE OF CONTENTS

CHAPTER 1: **Exchange of DNA-Data**

1. ***DNA related forensic issues, matching rules and algorithms***

1.1. *Properties of DNA-profiles*

The DNA profile may contain 24 pairs of numbers representing the alleles of 24 loci which are also used in the DNA-procedures of Interpol. The names of these loci are shown in the following table:

VWA	TH01	D21S11	FGA	D8S1179	D3S1358	D18S51	Amelogenin
TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539	D2S1338	D19S433
Penta D	Penta E	FES	F13A1	F13B	SE33	CD4	GABA

The seven grey loci in the top row are both the present European Standard Set (ESS) and the Interpol Standard Set of Loci (ISSOL).

Inclusion Rules:

The DNA-profiles made available by the Member States for searching and comparison as well as the DNA-profiles sent out for searching and comparison must contain at least six full designated ([1]) loci and may contain additional loci or blanks depending on their availability. The reference DNA profiles must contain at least six of the seven ESS of loci. In order to raise the accuracy of matches, all available alleles shall be stored in the indexed DNA profile database and be used for searching and comparison. Each Member State should implement as soon as practically possible any new ESS of loci adopted by the EU.

Mixed profiles are not allowed, so that the allele values of each locus will consist of only two numbers, which may be the same in the case of homozygosity at a given locus.

Wild-cards and Micro-variants are to be dealt with using the following rules:

— Any non-numerical value except amelogenin contained in the profile (e.g. 'o', 'f', 'r', 'na', 'nr' or 'un') has to be automatically converted for the export to a wild card (*) and searched against all,

— Numerical values '0', '1' or '99' contained in the profile have to be automatically converted for the export to a wild card (*) and searched against all,

— If three alleles are provided for one locus the first allele will be accepted and the remaining two alleles have to be automatically converted for the export to a wild card (*) and searched against all,

— When wild card values are provided for allele 1 or 2 then both permutations of the numerical value given for the locus will be searched (e.g. 12, * could match against 12,14 or 9,12),

— Pentanucleotide (Penta D, Penta E and CD4) micro-variants will be matched according to the following:

x.1 = x, x.1, x.2

x.2 = x.1, x.2, x.3

x.3 = x.2, x.3, x.4

x.4 = x.3, x.4, x + 1,

— Tetranucleotide (the rest of the loci are tetranucleotides) micro-variants will be matched according to the following:

x.1 = x, x.1, x.2

x.2 = x.1, x.2, x.3

x.3 = x.2, x.3, x + 1.

([1]) 'Full designated' means the handling of rare allelle values is included.

1.2. *Matching rules*

The comparison of two DNA-profiles will be performed on the basis of the loci for which a pair of allele values is available in both DNA-profiles. At least six full designated loci (exclusive of amelogenin) must match between both DNA-profiles before a hit response is provided.

A full match (Quality 1) is defined as a match, when all allele values of the compared loci commonly contained in the requesting and requested DNA-profiles are the same. A near match is defined as a match, when the value of only one of all the compared alleles is different in the two DNA profiles (Quality 2, 3 and 4). A near match is only accepted if there are at least six full designated matched loci in the two compared DNA profiles.

The reason for a near match may be:

— a human typing error at the point of entry of one of the DNA-profiles in the search request or the DNA-database,

— an allele-determination or allele-calling error during the generation procedure of the DNA-profile.

1.3. *Reporting rules*

Both full matches, near matches and 'no hits' will be reported.

The matching report will be sent to the requesting national contact point and will also be made available to the requested national contact point (to enable it to estimate the nature and number of possible follow-up requests for further available personal data and other information associated with the DNA-profile corresponding to the hit in accordance with Articles 5 and 10 of Decision 2008/615/JHA).

2. ***Member State code number table***

In accordance with Decision 2008/615/JHA, ISO 3166-1 alpha-2 code are used for setting up the domain names and other configuration parameters required in the Prüm DNA data exchange applications over a closed network.

ISO 3166-1 alpha-2 codes are the following two-letter Member State codes.

Member State names	Code	Member State names	Code
Belgium	BE	Luxembourg	LU
Bulgaria	BG	Hungary	HU
Czech Republic	CZ	Malta	MT
Denmark	DK	Netherlands	NL
Germany	DE	Austria	AT
Estonia	EE	Poland	PL
Greece	EL	Portugal	PT
Spain	ES	Romania	RO
France	FR	Slovakia	SK
Ireland	IE	Slovenia	SI
Italy	IT	Finland	FI
Cyprus	CY	Sweden	SE
Latvia	LV	United Kingdom	UK
Lithuania	LT		

3. ***Functional analysis***

3.1. *Availability of the system*

Requests pursuant to Article 3 of Decision 2008/615/JHA should reach the targeted database in the chronological order that each request was sent, responses should be dispatched to reach the requesting Member State within 15 minutes of the arrival of requests.

3.2. *Second step*

When a Member State receives a report of match, its national contact point is responsible for comparing the values of the profile submitted as a question and the values of the profile(s) received as an answer to validate and check the evidential value of the profile. National contact points can contact each other directly for validation purposes.

Legal assistance procedures start after validation of an existing match between two profiles, on the basis of a 'full match' or a 'near match' obtained during the automated consultation phase.

4. ***DNA interface control document***

4.1. *Introduction*

4.1.1. Objectives

This Chapter defines the requirements for the exchange of DNA profile information between the DNA database systems of all Member States. The header fields are defined specifically for the Prüm DNA exchange, the data part is based on the DNA profile data part in the XML schema defined for the Interpol DNA exchange gateway.

Data are exchanged by SMTP (Simple Mail Transfer Protocol) and other state-of-the-art technologies, using a central relay mail server provided by the network provider. The XML file is transported as mail body.

4.1.2. Scope

This ICD defines the content of the message (mail) only. All network-specific and mail-specific topics are defined uniformly in order to allow a common technical base for the DNA data exchange.

This includes:

— the format of the subject field in the message to enable/allow for an automated processing of the messages,

— whether content encryption is necessary and if yes which methods should be chosen,

— the maximum length of messages.

4.1.3. XML structure and principles

The XML message is structured into;

— header part, which contains information about the transmission, and

— data part, which contains profile specific information, as well as the profile itself.

The same XML schema shall be used for request and response.

For the purpose of complete checks of unidentified DNA profiles (Article 4 of Decision 2008/615/JHA) it shall be possible to send a batch of profiles in one message. A maximum number of profiles within one message must be defined. The number is depending from the maximum allowed mail size and shall be defined after selection of the mail server.

XML example:

<?version="1.0" standalone="yes"?>

<PRUEMDNAx xmlns:msxsl="urn:schemas-microsoft-com:xslt"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<header>

(…)

</header>

<datas>

(…)

</datas>

[<datas> datas structure repeated, if multiple profiles sent by (….) a single SMTP message, only allowed for Article 4 cases

</datas>]

</PRUEMDNA>

4.2. *XML structure definition*

The following definitions are for documentation purposes and better readability, the real binding information is provided by an XML schema file (PRUEM DNA.xsd).

4.2.1. Schema PRUEMDNAx

It contains the following fields:

Fields	Type	Description
header	PRUEM_header	Occurs: 1
datas	PRUEM_datas	Occurs: 1 … 500

4.2.2. Content of header structure

4.2.2.1. PRUEM header

This is a structure describing the XML file header. It contains the following fields:

Fields	Type	Description
direction	PRUEM_header_dir	Direction of message flow
ref	String	Reference of the XML file
generator	String	Generator of XML file
schema_version	String	Version number of schema to use
requesting	PRUEM_header_info	Requesting Member State info
requested	PRUEM_header_info	Requested Member State info

4.2.2.2. PRUEM_header dir

Type of data contained in message, value can be:

Value	Description
R	Request

Value	Description
A	Answer

4.2.2.3. PRUEM header info

Structure to describe Member State as well as message date/time. It contains the following fields:

Fields	Type	Description
source_isocode	String	ISO 3166-2 code of the requesting Member State
destination_isocode	String	ISO 3166-2 code of the requested Member State
request_id	String	unique Identifier for a request
date	Date	Date of creation of message
time	Time	Time of creation of message

4.2.3. Content of PRUEM Profile data

4.2.3.1. PRUEM_datas

This is a structure describing the XML profile data part. It contains the following fields:

Fields	Type	Description
reqtype	PRUEM request type	Type of request (Article 3 or 4)
date	Date	Date profile stored
type	PRUEM_datas_type	Type of profile
result	PRUEM_datas_result	Result of request
agency	String	Name of corresponding unit responsible for the profile
profile_ident	String	Unique Member State profile ID
message	String	Error Message, if result = E
profile	IPSG_DNA_profile	If direction = A (Answer) AND result ≠ H (Hit) empty
match_id	String	In case of a HIT PROFILE_ID of the requesting profile
quality	PRUEM_hitquality_type	Quality of Hit
hitcount	Integer	Count of matched Alleles
rescount	Integer	Count of matched profiles. If direction = R (Request), then empty. If quality!=0 (the original requested profile), then empty.

4.2.3.2. PRUEM_request_type

Type of data contained in message, value can be:

Value	Description
3	Requests pursuant to Article 3 of Decision 2008/615/JHA
4	Requests pursuant to Article 4 of Decision 2008/615/JHA

4.2.3.3. PRUEM_hitquality_type

Value	Description
0	Referring original requesting profile: Case 'No Hit': original requesting profile sent back only; Case 'Hit': original requesting profile and matched profiles sent back.
1	Equal in all available alleles without wildcards
2	Equal in all available alleles with wildcards
3	Hit with Deviation (Microvariant)
4	Hit with mismatch

4.2.3.4. PRUEM_data_type

Type of data contained in message, value can be:

Value	Description
P	Person profile
S	Stain

4.2.3.5. PRUEM_data_result

Type of data contained in message, value can be:

Value	Description
U	Undefined, If direction = R (request)
H	Hit
N	No Hit
E	Error

4.2.3.6. IPSG_DNA_profile

Structure describing a DNA profile. It contains the following fields:

Fields	Type	Description
ess_issol	IPSG_DNA_ISSOL	Group of loci corresponding to the ISSOL (standard group of Loci of Interpol)
additional_loci	IPSG_DNA_additional_loci	Other loci
marker	String	Method used to generate of DNA
profile_id	String	Unique identifier for DNA profile

4.2.3.7. IPSG_DNA_ISSOL

Structure containing the loci of ISSOL (Standard Group of Interpol loci). It contains the following fields:

Fields	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01

Fields	Type	Description
d21s11	IPSG_DNA_locus	Locus d21s11
fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
amelogenin	IPSG_DNA_locus	Locus amelogin

4.2.3.8. IPSG_DNA_additional_loci

Structure containing the other loci. It contains the following fields:

Fields	Type	Description
tpox	IPSG_DNA_locus	Locus tpox
csf1po	IPSG_DNA_locus	Locus csf1po
d13s317	IPSG_DNA_locus	Locus d13s317
d7s820	IPSG_DNA_locus	Locus d7s820
d5s818	IPSG_DNA_locus	Locus d5s818
d16s539	IPSG_DNA_locus	Locus d16s539
d2s1338	IPSG_DNA_locus	Locus d2s1338
d19s433	IPSG_DNA_locus	Locus d19s433
penta_d	IPSG_DNA_locus	Locus penta_d
penta_e	IPSG_DNA_locus	Locus penta_e
fes	IPSG_DNA_locus	Locus fes
f13a1	IPSG_DNA_locus	Locus f13a1
f13b	IPSG_DNA_locus	Locus f13b
se33	IPSG_DNA_locus	Locus se33
cd4	IPSG_DNA_locus	Locus cd4
gaba	IPSG_DNA_locus	Locus gaba

4.2.3.9. IPSG_DNA_locus

Structure describing a locus. It contains the following fields:

Fields	Type	Description
low_allele	String	Lowest value of an allele
high_allele	String	Highest value of an allele

5. *Application, security and communication architecture*

5.1. *Overview*

In implementing applications for the DNA data exchange within the framework of Decision 2008/615/JHA, a common communication network shall be used, which will be logically closed among the Member States. In order to exploit this common communication infrastructure of sending requests and receiving replies in a more

effective way, an asynchronous mechanism to convey DNA and dactyloscopic data requests in a wrapped SMTP e-mail message is adopted. In fulfilment of security concerns, the mechanism s/MIME as extension to the SMTP functionality will be used to establish a true end-to-end secure tunnel over the network.

The operational TESTA (Trans European Services for Telematics between Administrations) is used as the communication network for data exchange among the Member States. TESTA is under the responsibility of the European Commission. Taking into account that national DNA databases and the current national access points of TESTA may be located on different sites in the Member States, access to TESTA may be set up either by:

1. using the existing national access point or establishing a new national TESTA access point; or by

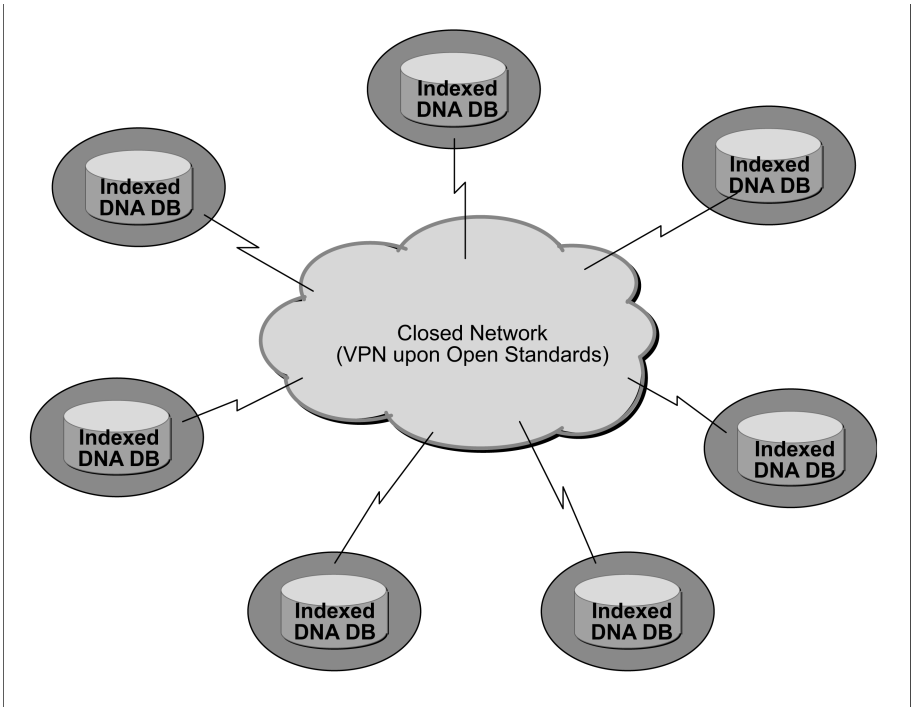
2. setting up a secure local link from the site where the DNA database is located and managed by the competent national agency to the existing national TESTA access point.

The protocols and standards deployed in the implementation of Decision 2008/615/JHA applications comply with the open standards and meet the requirements imposed by national security policy makers of the Member States.

5.2. *Upper Level Architecture*

In the scope of Decision 2008/615/JHA, each Member State will make its DNA data available to be exchanged with and/or searched by other Member States in conformity with the standardised common data format. The architecture is based upon an any-to-any communication model. There exists neither a central computer server nor a centralised database to hold DNA profiles.

Figure 1: Topology of DNA Data Exchange



In addition to the fulfilment of national legal constraints at Member States' sites, each Member State may decide what kind of hardware and software should be deployed for the configuration at its site to comply with the requirements set out in Decision 2008/615/JHA.

5.3. *Security Standards and Data Protection*

Three levels of security concerns have been considered and implemented.

5.3.1. Data Level

DNA profile data provided by each Member State have to be prepared in compliance with a common data protection standard, so that requesting Member States will receive an answer mainly to indicate HIT or NO-HIT along with an identification number in case of a HIT, which does not contain any personal information. The further investigation after the notification of a HIT will be conducted at bilateral level pursuant to the existing national legal and organisational regulations of the respective Member States' sites.

5.3.2. Communication Level

Messages containing DNA profile information (requesting and replying) will be encrypted by means of a state-of-the-art mechanism in conformity with open standards, such as s/MIME, before they are forwarded to the sites of other Member States.

5.3.3. Transmission Level

All encrypted messages containing DNA profile information will be forwarded onto other Member States' sites through a virtual private tunnelling system administered by a trusted network provider at the international level and the secure links to this tunnelling system under the national responsibility. This virtual private tunnelling system does not have a connection point with the open Internet.

5.4. *Protocols and Standards to be used for encryption mechanism: s/MIME and related packages*

The open standard s/MIME as extension to de facto e-mail standard SMTP will be deployed to encrypt messages containing DNA profile information. The protocol s/MIME (V3) allows signed receipts, security labels, and secure mailing lists and is layered on Cryptographic Message Syntax (CMS), an IETF specification for cryptographic protected messages. It can be used to digitally sign, digest, authenticate or encrypt any form of digital data.

The underlying certificate used by s/MIME mechanism has to be in compliance with X.509 standard. In order to ensure common standards and procedures with other Prüm applications, the processing rules for s/MIME encryption operations or to be applied under various COTS (Commercial Product of the Shelves) environments, are as follows:

— the sequence of the operations is: first encryption and then signing,

— the encryption algorithm AES (Advanced Encryption Standard) with 256 bit key length and RSA with 1 024 bit key length shall be applied for symmetric and asymmetric encryption respectively,

— the hash algorithm SHA-1 shall be applied.

s/MIME functionality is built into the vast majority of modern e-mail software packages including Outlook, Mozilla Mail as well as Netscape Communicator 4.x and inter-operates among all major e-mail software packages.

Because of s/MIME's easy integration into national IT infrastructure at all Member States' sites, it is selected as a viable mechanism to implement the communication security level. For achieving the goal 'Proof of Concept' in a more efficient way and reducing costs the open standard JavaMail API is however chosen for prototyping DNA data exchange. JavaMail API provides simple encryption and decryption of e-mails using s/MIME and/or OpenPGP. The intent is to provide a single, easy-to-use API for e-mail clients that want to send and received encrypted e-mail in either of the two most popular e-mail encryption formats. Therefore any state-of-the-art implementations to JavaMail API will suffice for the requirements set by Decision 2008/615/JHA, such as the product of Bouncy Castle JCE (Java Cryptographic Extension), which will be used to implement s/MIME for prototyping DNA data exchange among all Member States.

5.5. *Application Architecture*

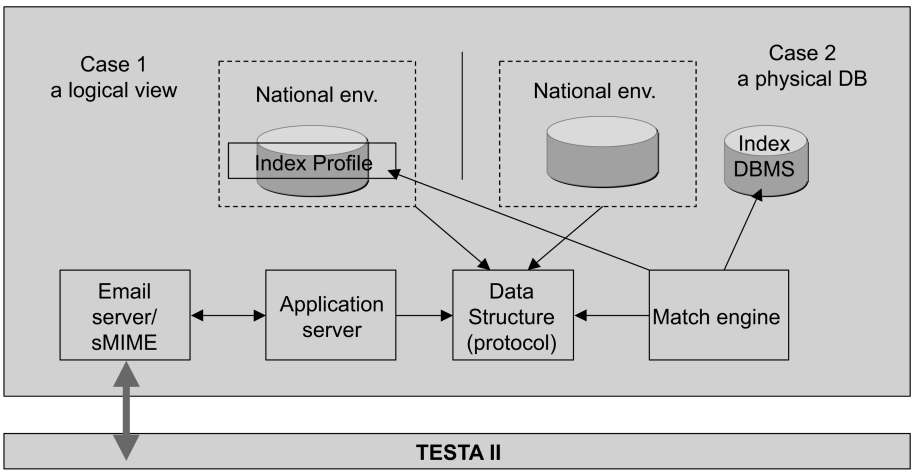
Each Member State will provide the other Member States with a set of standardised DNA profile data which are in conformity with the current common ICD. This can be done either by providing a logical view over individual national database or by establishing a physical exported database (indexed database).

The four main components: E-mail server/s/MIME, Application Server, Data Structure Area for fetching/feeding data and registering incoming/outgoing messages, and Match Engine implement the whole application logic in a product-independent way.

In order to provide all Member States with an easy integration of the components into their respective national sites, the specified common functionality has been implemented by means of open source components, which could be selected by each Member State depending on its national IT policy and regulations. Because of the independent features to be implemented to get access to indexed databases containing DNA profiles covered by Decision 2008/615/JHA, each Member State can freely select its hardware and software platform, including database and operating systems.

A prototype for the DNA Data Exchange has been developed and successfully tested over the existing common network. The version 1.0 has been deployed in the productive environment and is used for daily operations. Member States may use the jointly developed product but may also develop their own products. The common product components will be maintained, customised and further developed according to changing IT, forensic and/or functional police requirements.

Figure 2: Overview Application Topology



5.6. *Protocols and Standards to be used for application architecture:*

5.6.1. XML

The DNA data exchange will fully exploit XML-schema as attachment to SMTP e-mail messages. The eXtensible Markup Language (XML) is a W3C-recommended general-purpose markup language for creating special-purpose markup languages, capable of describing many different kinds of data. The description of the DNA profile suitable for exchange among all Member States has been done by means of XML and XML schema in the ICD document.

5.6.2. ODBC

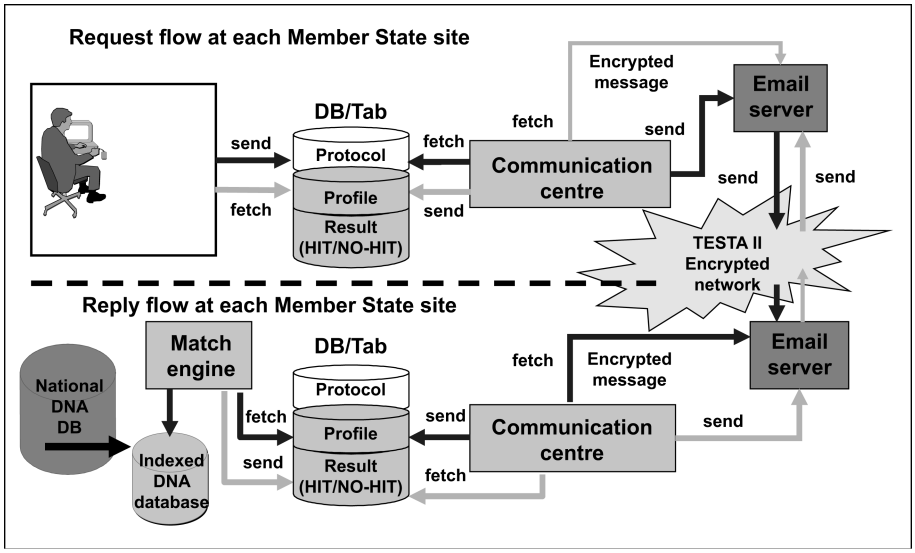
Open DataBase Connectivity provides a standard software API method for accessing database management systems and making it independent of programming languages, database and operating systems. ODBC has, however, certain drawbacks. Administering a large number of client machines can involve a diversity of drivers and DLLs. This complexity can increase system administration overhead.

5.6.3. JDBC

Java DataBase Connectivity (JDBC) is an API for the Java programming language that defines how a client may access a database. In contrast to ODBC, JDBC does not require to use a certain set of local DLLs at the Desktop.

The business logic to process DNA profile requests and replies at each Member States' site is described in the following diagram. Both requesting and replying flows interact with a neutral data area comprising different data pools with a common data structure.

Figure 3: Overview Application Workflow at each Member State's site



5.7. *Communication Environment*

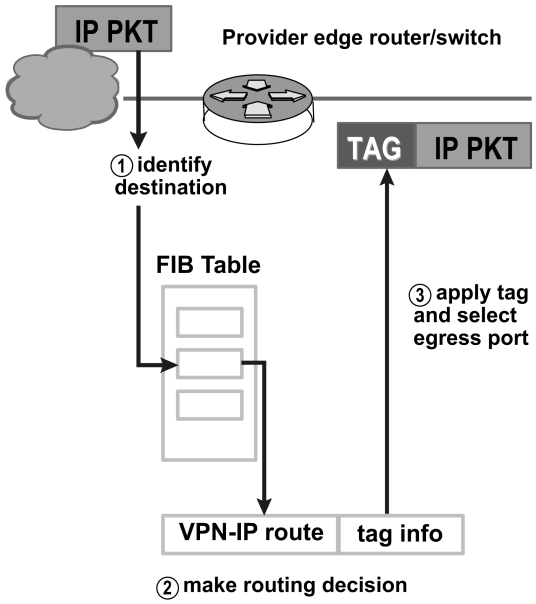
5.7.1. Common Communication Network: TESTA and its follow-up infrastructure

The application DNA data exchange will exploit the e-mail, an asynchronous mechanism, to send requests and to receive replies among the Member States. As all Member States have at least one national access point to the TESTA network, the DNA data exchange will be deployed over the TESTA network. TESTA provides a number of added-value services through its e-mail relay. In addition to hosting TESTA specific e-mail boxes, the infrastructure can implement mail distribution lists and routing policies. This allows TESTA to be used as a clearing house for messages addressed to administrations connected to the EU wide Domains. Virus check mechanisms may also be put in place.

The TESTA e-mail relay is built on a high availability hardware platform located at the central TESTA application facilities and protected by firewall. The TESTA Domain Name Services (DNS) will resolve resource locators to IP addresses and hide addressing issues from the user and from applications.

5.7.2. Security Concern

The concept of a VPN (Virtual Private Network) has been implemented within the framework of TESTA. Tag Switching Technology used to build this VPN will evolve to support Multi-Protocol Label Switching (MPLS) standard developed by the Internet Engineering Task Force (IETF).



MPLS is an IETF standard technology that speeds up network traffic flow by avoiding packet analysis by intermediate routers (hops). This is done on the basis of so-called labels that are attached to packet by the edge routers of the backbone, on the basis of information stored in the forwarding information base (FIB). Labels are also used to implement virtual private networks (VPNs).

MPLS combines the benefits of layer 3 routing with the advantages of layer 2 switching. Because IP addresses are not evaluated during transition through the backbone, MPLS does not impose any IP addressing limitations.

Furthermore e-mail messages over the TESTA will be protected by s/MIME driven encryption mechanism. Without knowing the key and possessing the right certificate, nobody can decrypt messages over the network.

5.7.3. Protocols and Standards to be used over the communication network

5.7.3.1. SMTP

Simple Mail Transfer Protocol is the de facto standard for e-mail transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and then the message text is transferred. SMTP uses TCP port 25 upon the specification by the IETF. To determine the SMTP server for a given domain name, the MX (Mail eXchange) DNS (Domain Name Systems) record is used.

Since this protocol started as purely ASCII text-based it did not deal well with binary files. Standards such as MIME were developed to encode binary files for transfer through SMTP. Today, most SMTP servers support the 8BITMIME and s/MIME extension, permitting binary files to be transmitted almost as easily as plain text. The processing rules for s/MIME operations are described in the section s/MIME (see Chapter 5.4).

SMTP is a 'push' protocol that does not allow one to 'pull' messages from a remote server on demand. To do this a mail client must use POP3 or IMAP. Within the framework of implementing DNA data exchange it is decided to use the protocol POP3.

5.7.3.2. POP

Local e-mail clients use the Post Office Protocol version 3 (POP3), an application-layer Internet standard protocol, to retrieve e-mail from a remote server over a TCP/IP connection. By using the SMTP Submit profile of the SMTP protocol, e-mail clients send messages across the Internet or over a corporate network. MIME serves as the standard for attachments and non-ASCII text in e-mail. Although neither POP3 nor SMTP requires MIME-formatted e-mail, essentially Internet e-mail comes MIME-formatted, so POP clients must also understand and use MIME. The whole communication environment of Decision 2008/615/JHA will therefore include the components of POP.

5.7.4. Network Address Assignment

Operative environment

A dedicated block of C class subnet has currently been allocated by the European IP registration authority (RIPE) to TESTA. Further address blocks may be allocated to TESTA in the future if required. The assignment of IP addresses to Member States is based upon a geographical schema in Europe. The data exchange among Member States within the framework of Decision 2008/615/JHA is operated over a European wide logically closed IP network.

Testing Environment

In order to provide a smooth running environment for the daily operation among all connected Member States, it is necessary to establish a testing environment over the closed network for new Member States which prepare to join the operations. A sheet of parameters including IP addresses, network settings, e-mail domains as well as application user accounts has been specified and should be set up at the corresponding Member State's site. Moreover, a set of pseudo DNA profiles has been constructed for the test purposes.

5.7.5. Configuration Parameters

A secure e-mail system is set up using the eu-admin.net domain. This domain with the associated addresses will not be accessible from a location not on the TESTA EU wide domain, because the names are only known on the TESTA central DNS server, which is shielded from the Internet.

The mapping of these TESTA site addresses (host names) to their IP addresses is done by the TESTA DNS service. For each Local Domain, a Mail entry will be added to this TESTA central DNS server, relaying all e-mail messages sent to TESTA Local Domains to the TESTA central Mail Relay. This TESTA central Mail Relay will then forward them to the specific Local Domain e-mail server using the Local Domain e-mail addresses. By relaying the e-mail in this way, critical information contained in e-mails will only pass the Europe - wide closed network infrastructure and not the insecure Internet.

It is necessary to establish sub-domains (***bold italics***) at the sites of all Member States upon the following syntax:

'***application-type*.pruem.*Member State-code*.**eu-admin.net', where:

'***Member State-code***' takes the value of one of the two letter-code Member State codes (i.e. AT, BE, etc.).

'***application-type***' takes one of the values: DNA and FP.

By applying the above syntax, the sub domains for the Member States are shown in the following table:

MS	Sub Domains	Comments
BE	***dna*.pruem.be**.eu-admin.net	Setting up a secure local link to the existing TESTA II access point
	***fp*.pruem.be**.eu-admin.net	
BG	***dna*.pruem.bg**.eu-admin.net	
	***fp*.pruem.bg**.eu-admin.net	
CZ	***dna*.pruem.cz**.eu-admin.net	
	***fp*.pruem.cz**.eu-admin.net	
DK	***dna*.pruem.dk**.eu-admin.net	
	***fp*.pruem.dk**.eu-admin.net	
DE	***dna*.pruem.de**.eu-admin.net	Using the existing TESTA II national access points
	***fp*.pruem.de**.eu-admin.net	
EE	***dna*.pruem.ee**.eu-admin.net	
	***fp*.pruem.ee**.eu-admin.net	

MS	Sub Domains	Comments
IE	***dna*.pruem.ie**.eu-admin.net	
	***fp*.pruem.ie**.eu-admin.net	
EL	***dna*.pruem.el**.eu-admin.net	
	***fp*.pruem.el**.eu-admin.net	
ES	***dna*.pruem.es**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.es**.eu-admin.net	
FR	***dna*.pruem.fr**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.fr**.eu-admin.net	
IT	***dna*.pruem.it**.eu-admin.net	
	***fp*.pruem.it**.eu-admin.net	
CY	***dna*.pruem.cy**.eu-admin.net	
	***fp*.pruem.cy**.eu-admin.net	
LV	***dna*.pruem.lv**.eu-admin.net	
	***fp*.pruem.lv**.eu-admin.net	
LT	***dna*.pruem.lt**.eu-admin.net	
	***fp*.pruem.lt**.eu-admin.net	
LU	***dna*.pruem.lu**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.lu**.eu-admin.net	
HU	***dna*.pruem.hu**.eu-admin.net	
	***fp*.pruem.hu**.eu-admin.net	
MT	***dna*.pruem.mt**.eu-admin.net	
	***fp*.pruem.mt**.eu-admin.net	
NL	***dna*.pruem.nl**.eu-admin.net	Intending to establish a new TESTA II access point at the NFI
	***fp*.pruem.nl**.eu-admin.net	
AT	***dna*.pruem.at**.eu-admin.net	Using the existing TESTA II national access point
	***fp*.pruem.at**.eu-admin.net	
PL	***dna*.pruem.pl**.eu-admin.net	
	***fp*.pruem.pl**.eu-admin.net	
PT	***dna*.pruem.pt**.eu-admin.net	……
	***fp*.pruem.pt**.eu-admin.net	……
RO	***dna*.pruem.ro**.eu-admin.net	
	***fp*.pruem.ro**.eu-admin.net	

MS	Sub Domains	Comments
SI	***dna*.pruem.si**.eu-admin.net	……
	***fp*.pruem.si**.eu-admin.net	……
SK	***dna*.pruem.sk**.eu-admin.net	
	***fp*.pruem.sk**.eu-admin.net	
FI	***dna*.pruem.fi**.eu-admin.net	*[To be inserted]*
	***fp*.pruem.fi**.eu-admin.net	
SE	***dna*.pruem.se**.eu-admin.net	
	***fp*.pruem.se**.eu-admin.net	
UK	***dna*.pruem.uk**.eu-admin.net	
	***fp*.pruem.uk**.eu-admin.net	

CHAPTER 2: **Exchange of dactyloscopic data (interface control document)**

The purpose of the following document interface Control Document is to define the requirements for the exchange of dactyloscopic information between the Automated Fingerprint Identification Systems (AFIS) of the Member States. It is based on the Interpol-Implementation of ANSI/NIST-ITL 1-2000 (INT-I, Version 4.22b).

This version shall cover all basic definitions for Logical Records Type-1, Type-2, Type-4, Type-9, Type-13 and Type-15 required for image and minutiæ based dactyloscopic processing.

1. ***File Content Overview***

A dactyloscopic file consists of several logical records. There are sixteen types of record specified in the original ANSI/NIST-ITL 1-2000 standard. Appropriate ASCII separation characters are used between each record and the fields and subfields within the records.

Only 6 record types are used to exchange information between the originating and the destination agency:

Type-1 → Transaction information

Type-2 → Alphanumeric persons/case data

Type-4 → High resolution greyscale dactyloscopic images

Type-9 → Minutiæ Record

Type-13 → Variable resolution latent image record

Type-15 → Variable resolution palmprint image record

1.1. *Type-1 — File header*

This record contains routing information and information describing the structure of the rest of the file. This record type also defines the types of transaction which fall under the following broad categories:

1.2. *Type-2 — Descriptive text*

This record contains textual information of interest to the sending and receiving agencies.

1.3. *Type-4 — High resolution greyscale image*

This record is used to exchange high resolution greyscale (eight bit) dactyloscopic images sampled at 500 pixels/inch. The dactyloscopic images shall be compressed using the WSQ algorithm with a ratio of not more than 15:1. Other compression algorithms or uncompressed images must not be used.

1.4. *Type-9 — Minutiæ record*

Type-9 records are used to exchange ridge characteristics or minutiæ data. Their purpose is partly to avoid unnecessary duplication of AFIS encoding processes and partly to allow the transmission of AFIS codes which contain less data than the corresponding images.

1.5. *Type-13 — Variable-Resolution Latent Image Record*

This record shall be used to exchange variable-resolution latent fingerprint and latent palmprint images together with textural alphanumerical information. The scanning resolution of the images shall be 500 pixels/inch with 256 grey-levels. If the quality of the latent image is sufficient it shall be compressed using WSQ-algorithm. If necessary the resolution of the images may be expanded to more than 500 pixels/inch and more than 256 grey-levels on bilateral agreement. In this case, it is strongly recommended to use JPEG 2000 (see Appendix 7).

1.6. *Variable-Resolution Palmprint Image Record*

Type-15 tagged field image records shall be used to exchange variable-resolution palmprint images together with textural alphanumerical information. The scanning resolution of the images shall be 500 pixels/inch with 256 grey-levels. To minimise the amount of data all palmprint images shall be compressed using WSQ-algorithm. If necessary the resolution of the images may be expanded to more than 500 pixels/inch and more than 256 grey-levels on bilateral agreement. In this case, it is strongly recommended to use JPEG 2000 (see Appendix 7).

2. ***Record format***

A transaction file shall consist of one or more logical records. For each logical record contained in the file, several information fields appropriate to that record type shall be present. Each information field may contain one or more basic single-valued information items. Taken together these items are used to convey different aspects of the data contained in that field. An information field may also consist of one or more information items grouped together and repeated multiple times within a field. Such a group of information items is known as a subfield. An information field may therefore consist of one or more subfields of information items.

2.1. *Information separators*

In the tagged-field logical records, mechanisms for delimiting information are implemented by use of four ASCII information separators. The delimited information may be items within a field or subfield, fields within a logical record, or multiple occurrences of subfields. These information separators are defined in the standard ANSI X3.4. These characters are used to separate and qualify information in a logical sense. Viewed in a hierarchical relationship, the File Separator 'FS' character is the most inclusive followed by the Group Separator 'GS', the Record Separator 'RS', and finally the Unit Separator 'US' characters. Table 1 lists these ASCII separators and a description of their use within this standard.

Information separators should be functionally viewed as an indication of the type data that follows. The 'US' character shall separate individual information items within a field or subfield. This is a signal that the next information item is a piece of data for that field or subfield. Multiple subfields within a field separated by the 'RS' character signals the start of the next group of repeated information item(s). The 'GS' separator character used between information fields signals the beginning of a new field preceding the field identifying number that shall appear. Similarly, the beginning of a new logical record shall be signalled by the appearance of the 'FS' character.

The four characters are only meaningful when used as separators of data items in the fields of the ASCII text records. There is no specific meaning attached to these characters occurring in binary image records and binary fields — they are just part of the exchanged data.

Normally, there should be no empty fields or information items and therefore only one separator character should appear between any two data items. The exception to this rule occurs for those instances where the data in fields or information items in a transaction are unavailable, missing, or optional, and the processing of the transaction is not dependent upon the presence of that particular data. In those instances, multiple and adjacent separator characters shall appear together rather than requiring the insertion of dummy data between separator characters.

For the definition of a field that consists of three information items, the following applies. If the information for the second information item is missing, then two adjacent 'US' information separator characters would occur between the first and third information items. If the second and third information items were both missing, then three separator characters should be used — two 'US' characters in addition to the terminating field or subfield separator character. In general, if one or more mandatory or optional information items are unavailable for a field or subfield, then the appropriate number of separator character should be inserted.

It is possible to have side-by-side combinations of two or more of the four available separator characters. When data are missing or unavailable for information items, subfields, or fields, there must be one separator character less than the number of data items, subfields, or fields required.

Table 1: Separators Used

Code	Type	Description	Hexadecimal Value	Decimal Value
US	Unit Separator	Separates information items	1F	31
RS	Record Separator	Separates subfields	1E	30
GS	Group Separator	Separates fields	1D	29
FS	File Separator	Separates logical records	1C	28

2.2. *Record layout*

For tagged-field logical records, each information field that is used shall be numbered in accordance with this standard. The format for each field shall consist of the logical record type number followed by a period '.', a field number followed by a colon ':', followed by the information appropriate to that field. The tagged-field number can be any one-to-nine digit number occurring between the period '.' and the colon ':'. It shall be interpreted as an unsigned integer field number. This implies that a field number of '2.123:' is equivalent to and shall be interpreted in the same manner as a field number of '2.000000123:'.

For purposes of illustration throughout this document, a three-digit number shall be used for enumerating the fields contained in each of the tagged-field logical records described herein. Field numbers will have the form of 'TT.xxx:' where the 'TT' represents the one- or two-character record type followed by a period. The next three characters comprise the appropriate field number followed by a colon. Descriptive ASCII information or the image data follows the colon.

Logical Type-1 and Type-2 records contain only ASCII textual data fields. The entire length of the record (including field numbers, colons, and separator characters) shall be recorded as the first ASCII field within each of these record types. The ASCII File Separator 'FS' control character (signifying the end of the logical record or transaction) shall follow the last byte of ASCII information and shall be included in the length of the record.

In contrast to the tagged-field concept, the Type-4 record contains only binary data recorded as ordered fixed-length binary fields. The entire length of the record shall be recorded in the first four-byte binary field of each record. For this binary record, neither the record number with its period, nor the field identifier number and its following colon, shall be recorded. Furthermore, as all the field lengths of this record is either fixed or specified, none of the four separator characters ('US', 'RS', 'GS', or 'FS') shall be interpreted as anything other than binary data. For the binary record, the 'FS' character shall not be used as a record separator or transaction terminating character.

3. ***Type-1 Logical Record: the File Header***

This record describes the structure of the file, the type of the file, and other important information. The character set used for Type-1 fields shall contain only the 7-bit ANSI code for information interchange.

3.1. *Fields for Type-1 Logical Record*

3.1.1. Field 1.001: Logical Record Length (LEN)

This field contains the total count of the number of bytes in the whole Type-1 logical record. The field begins with '1.001:', followed by the total length of the record including every character of every field and the information separators.

3.1.2. Field 1.002: Version Number (VER)

To ensure that users know which version of the ANSI/NIST standard is being used, this four byte field specifies the version number of the standard being implemented by the software or system creating the file. The first two bytes specify the major version reference number, the second two the minor revision number. For example, the original 1986 Standard would be considered the first version and designated '0100' while the present ANSI/NIST-ITL 1-2000 standard is '0300'.

3.1.3. Field 1.003: File Content (CNT)

This field lists each of the records in the file by record type and the order in which the records appear in the logical file. It consists of one or more subfields, each of which in turn contains two information items describing a single logical record found in the current file. The subfields are entered in the same order in which the records are recorded and transmitted.

The first information item in the first subfield is '1', to refer to this Type-1 record. It is followed by a second information item which contains the number of other records contained in the file. This number is also equal to the count of the remaining subfields of field 1.003.

Each of the remaining subfields is associated with one record within the file, and the sequence of subfields corresponds to the sequence of records. Each subfield contains two items of information. The first is to identify the Type of the record. The second is the record's IDC. The 'US' character shall be used to separate the two information items.

3.1.4. Field 1.004: Type of Transaction (TOT)

This field contains a three letter mnemonic designating the type of the transaction. These codes may be different from those used by other implementations of the ANSI/NIST standard.

CPS: Criminal Print-to-Print Search. This transaction is a request for a search of a record relating to a criminal offence against a prints database. The person's prints must be included as WSQ-compressed images in the file.

In case of a No-HIT, the following logical records will be returned:

— 1 Type-1 Record,

— 1 Type-2 Record.

In case of a HIT, the following logical records will be returned:

— 1 Type-1 Record,

— 1 Type-2 Record,

— 1-14 Type-4 Record.

The CPS TOT is summarised in Table A.6.1 (Appendix 6).

PMS: Print-to-Latent Search. This transaction is used when a set of prints shall to be searched against an Unidentified Latent database. The response will contain the Hit/No-Hit decision of the destination AFIS search. If multiple unidentified latents exist, multiple SRE transactions will be returned, with one latent per transaction. The person's prints must be included as WSQ-compressed images in the file.

In case of a No-HIT, the following logical records will be returned:

— 1 Type-1 Record,

— 1 Type-2 Record.

In case of a HIT, the following logical records will be returned:

— 1 Type-1 Record,

— 1 Type-2 Record,

— 1 Type-13 Record.

The PMS TOT is summarised in Table A.6.1 (Appendix 6).

MPS: Latent-to-Print Search. This transaction is used when a latent is to be searched against a Prints database. The latent minutiæ information and the image (WSQ-compressed) must be included in the file.

In case of a No-HIT, the following logical records will be returned:

— 1 Type-1 Record,

— 1 Type-2 Record.

In case of a HIT, the following logical records will be returned:

— 1 Type-1 Record,

— 1 Type-2 Record,

— 1 Type-4 or Type-15 Record.

The MPS TOT is summarised in Table A.6.4 (Appendix 6).

MMS: Latent-to-Latent Search. In this transaction the file contains a latent which is to be searched against an Unidentified Latent database in order to establish links between various scenes of crime. The latent minutiæ information and the image (WSQ-compressed) must be included in the file.

In case of a No-HIT, the following logical records will be returned:

— 1 Type-1 Record,

— 1 Type-2 Record.

In case of a HIT, the following logical records will be returned:

— 1 Type-1 Record,

— 1 Type-2 Record,

— 1 Type-13 Record.

The MMS TOT is summarised in Table A.6.4 (Appendix 6).

SRE: This transaction is returned by the destination agency in response to dactyloscopic submissions. The response will contain the Hit/No-Hit decision of the destination AFIS search. If multiple candidates exist, multiple SRE transactions will be returned, with one candidate per transaction.

The SRE TOT is summarised in Table A.6.2 (Appendix 6).

ERR: This transaction is returned by the destination AFIS to indicate a transaction error. It includes a message field (ERM) indicating the error detected. The following logical records will be returned:

— 1 Type-1 Record,

— 1 Type-2 Record.

The ERR TOT is summarised in Table A.6.3 (Appendix 6).

Table 2: Permissible Codes in Transactions

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
CPS	M	M	M	—	—	—
SRE	M	M	C	— (C in case of latent hits)	C	C
MPS	M	M	—	M (1*)	M	—

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
MMS	M	M	—	M (1*)	M	—
PMS	M	M	M*	—	—	M*
ERR	M	M	—	—	—	—

Key:

M = Mandatory,
M* = Only one of both record-types may be included,
O = Optional,
C = Conditional on whether data is available,
— = Not allowed,
1* = Conditional depending on legacy systems.

3.1.5. Field 1.005: Date of Transaction (DAT)

This field indicates the date on which the transaction was initiated and must conform to the ISO standard notation of: YYYYMMDD

where YYYY is the year, MM is the month and DD is the day of the month. Leading zeros are used for single figure numbers. For example, '19931004' represents 4 October 1993.

3.1.6. Field 1.006: Priority (PRY)

This optional field defines the priority, on a level of 1 to 9, of the request. '1' is the highest priority and '9' the lowest. Priority '1' transactions shall be processed immediately.

3.1.7. Field 1.007: Destination Agency Identifier (DAI)

This field specifies the destination agency for the transaction.

It consists of two information items in the following format: CC/agency.

The first information item contains the Country Code, defined in ISO 3166, two alpha-numeric characters long. The second item, *agency*, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

3.1.8. Field 1.008: Originating Agency Identifier (ORI)

This field specifies the file originator and has the same format as the DAI (Field 1.007).

3.1.9. Field 1.009: Transaction Control Number (TCN)

This is a control number for reference purposes. It should be generated by the computer and have the following format: YYSSSSSSSSA

where YY is the year of the transaction, SSSSSSSS is an eight-digit serial number, and A is a check character generated by following the procedure given in Appendix 2.

Where a TCN is not available, the field, YYSSSSSSSS, is filled with zeros and the check character generated as above.

3.1.10. Field 1.010: Transaction Control Response (TCR)

Where a request was sent out, to which this is the response, this optional field will contain the transaction control number of the request message. It therefore has the same format as TCN (Field 1.009).

3.1.11. Field 1.011: Native Scanning Resolution (NSR)

This field specifies the normal scanning resolution of the system supported by the originator of the transaction. The resolution is specified as two numeric digits followed by the decimal point and then two more digits.

For all transactions pursuant to Decision 2008/615/JHA the sampling rate shall be 500 pixels/inch or 19,68 pixels/mm.

3.1.12. Field 1.012: Nominal Transmitting Resolution (NTR)

This five-byte field specifies the nominal transmitting resolution for the images being transmitted. The resolution is expressed in pixels/mm in the same format as NSR (Field 1.011).

3.1.13. Field 1.013: Domain name (DOM)

This mandatory field identifies the domain name for the user-defined Type-2 logical record implementation. It consists of two information items and shall be 'INT-I{US}4.22{GS}'.

3.1.14. Field 1.014: Greenwich mean time (GMT)

This mandatory field provides a mechanism for expressing the date and time in terms of universal Greenwich Mean Time (GMT) units. If used, the GMT field contains the universal date that will be in addition to the local date contained in Field 1.005 (DAT). Use of the GMT field eliminates local time inconsistencies encountered when a transaction and its response are transmitted between two places separated by several time zones. The GMT provides a universal date and 24-hour clock time independent of time zones. It is represented as 'CCYYMMDDHHMMSSZ', a 15-character string that is the concatenation of the date with the GMT and concludes with a 'Z'. The 'CCYY' characters shall represent the year of the transaction, the 'MM' characters shall be the tens and units values of the month, and the 'DD' characters shall be the tens and units values of the day of the month, the 'HH' characters represent the hour, the 'MM' the minute, and the 'SS' represents the second. The complete date shall not exceed the current date.

4. ***Type-2 Logical Record: Descriptive Text***

The structure of most of this record is not defined by the original ANSI/NIST standard. The record contains information of specific interest to the agencies sending or receiving the file. To ensure that communicating dactyloscopic systems are compatible, it is required that only the fields listed below are contained within the record. This document specifies which fields are mandatory and which optional, and also defines the structure of the individual fields.

4.1. *Fields for Type-2 Logical Record*

4.1.1. Field 2.001: Logical Record Length (LEN)

This mandatory field contains the length of this Type-2 record, and specifies the total number of bytes including every character of every field contained in the record and the information separators.

4.1.2. Field 2.002: Image Designation Character (IDC)

The IDC contained in this mandatory field is an ASCII representation of the IDC as defined in the File Content field (CNT) of the Type-1 record (Field 1.003).

4.1.3. Field 2.003: System Information (SYS)

This field is mandatory and contains four bytes which indicate which version of the INT-I this particular Type-2 record complies with.

The first two bytes specify the major version number, the second two the minor revision number. For example, this implementation is based on INT-I version 4 revision 22 and would be represented as '0422'.

4.1.4. Field 2.007: Case Number (CNO)

This is a number assigned by the local dactyloscopic bureau to a collection of latents found at a scene-of-crime. The following format is adopted: CC/number

where CC is the Interpol Country Code, two alpha-numeric characters in length, and the number complies with the appropriate local guidelines and may be up to 32 alpha-numeric characters long.

This field allows the system to identify latents associated with a particular crime.

4.1.5. Field 2.008: Sequence Number (SQN)

This specifies each sequence of latents within a case. It can be up to four numeric characters long. A sequence is a latent or series of latents which are grouped together for the purposes of filing and/or searching. This definition implies that even single latents will still have to be assigned a sequence number.

This field together with MID (Field 2.009) may be included to identify a particular latent within a sequence.

4.1.6. Field 2.009: Latent Identifier (MID)

This specifies the individual latent within a sequence. The value is a single letter or two letters, with 'A' assigned to the first latent, 'B' to the second, and so on up to a limit of 'ZZ'. This field is used analogue to the latent sequence number discussed in the description for SQN (Field 2.008).

4.1.7. Field 2.010: Criminal Reference Number (CRN)

This is a unique reference number assigned by a national agency to an individual who is charged for the first time with committing an offence. Within one country no individual ever has more than one CRN, or shares it with any other individual. However, the same individual may have Criminal Reference Numbers in several countries, which will be distinguishable by means of the country code.

The following format is adopted for CRN field: CC/number

where CC is the Country Code, defined in ISO 3166, two alpha-numeric characters in length, and the number complies with the appropriate national guidelines of the issuing agency, and may be up to 32 alpha-numeric characters long.

For transactions pursuant to Decision 2008/615/JHA this field will be used for the national criminal reference number of the originating agency which is linked to the images in Type-4 or Type-15 Records.

4.1.8. Field 2.012: Miscellaneous Identification Number (MN1)

This fields contains the CRN (Field 2.010) transmitted by a CPS or PMS transaction without the leading country code.

4.1.9. Field 2.013: Miscellaneous Identification Number (MN2)

This fields contains the CNO (Field 2.007) transmitted by an MPS or MMS transaction without the leading country code.

4.1.10. Field 2.014: Miscellaneous Identification Number (MN3)

This fields contains the SQN (Field 2.008) transmitted by an MPS or MMS transaction.

4.1.11. Field 2.015: Miscellaneous Identification Number (MN4)

This fields contains the MID (Field 2.009) transmitted by an MPS or MMS transaction.

4.1.12. Field 2.063: Additional Information (INF)

In case of an SRE transaction to a PMS request this field gives information about the finger which caused the possible HIT. The format of the field is:

NN where *NN* is the finger position code defined in table 5, two digits in length.

In all other cases the field is optional. It consists of up to 32 alpha-numeric characters and may give additional information about the request.

4.1.13. Field 2.064: Respondents List (RLS)

This field contains at least two subfields. The first subfield describes the type of search that has been carried out, using the three-letter mnemonics which specify the transaction type in TOT (Field 1.004). The second subfield contains a single character. An 'I' shall be used to indicate that a HIT has been found and an 'N' shall be used to indicate that no matching cases have been found (NOHIT). The third subfield contains the sequence identifier for the candidate result and the total number of candidates separated by a slash. Multiple messages will be returned if multiple candidates exist.

In case of a possible HIT the fourth subfield shall contain the score up to six digits long. If the HIT has been verified the value of this subfield is defined as '999999'.

Example: 'CPS{RS}I{RS}001/001{RS}999999{GS}'

If the remote AFIS does not assign scores, then a score of zero should be used at the appropriate point.

4.1.14. Field 2.074: Status/Error Message Field (ERM)

This field contains error messages resulting from transactions, which will be sent back to the requester as part of an Error Transaction.

Table 3: Error messages

Numeric code (1-3)	Meaning (5-128)
003	ERROR: UNAUTHORISED ACCESS
101	Mandatory field missing
102	Invalid record type
103	Undefined field
104	Exceed the maximum occurrence
105	Invalid number of subfields
106	Field length too short
107	Field length too long
108	Field is not a number as expected
109	Field number value too small
110	Field number value too big
111	Invalid character
112	Invalid date
115	Invalid item value
116	Invalid type of transaction
117	Invalid record data
201	ERROR: INVALID TCN
501	ERROR: INSUFFICIENT FINGERPRINT QUALITY
502	ERROR: MISSING FINGERPRINTS
503	ERROR: FINGERPRINT SEQUENCE CHECK FAILED
999	ERROR: ANY OTHER ERROR. FOR FURTHER DETAILS CALL DESTINATION AGENCY.

Error messages in the range between 100 and 199:

These error messages are related to the validation of the ANSI/NIST records and defined as:

<error_code 1>: IDC <idc_number 1> FIELD <field_id 1> <dynamic text 1> LF

<error_code 2>: IDC <idc_number 2> FIELD <field_id 2> <dynamic text 2>…

where

— error_code is a code uniquely related to a specific reason (see table 3),

— field_id is the ANSI/NIST field number of the incorrect field (e.g. 1.001, 2.001, …) in the format <record_type>.<field_id>.<sub_field_id>,

— dynamic text is a more detailed dynamic description of the error,

— LF is a Line Feed separating errors if more then one error is encountered,

— for type-1 record the ICD is defined as '-1'.

Example:

201: IDC - 1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION

This field is mandatory for error transactions.

4.1.15. Field 2.320: Expected Number of Candidates (ENC)

This field contains the maximum number of candidates for verification expected by the requesting agency. The value of ENC must not exceed the values defined in table 11.

5. ***Type-4 Logical Record: High Resolution GreyScale Image***

It should be noted that Type-4 records are binary rather than ASCII in nature. Therefore each field is assigned a specific position within the record, which implies that all fields are mandatory.

The standard allows both image size and resolution to be specified within the record. It requires Type-4 Logical Records to contain dactyloscopic image data that are being transmitted at a nominal pixel density of 500 to 520 pixels per inch. The preferred rate for new designs is at a pixel density of 500 pixels per inch or 19,68 pixels per mm. 500 pixels per inch is the density specified by the INT-I, except that similar systems may communicate with each other at a non-preferred rate, within the limits of 500 to 520 pixels per inch.

5.1. *Fields for Type-4 Logical Record*

5.1.1. Field 4.001: Logical Record Length (LEN)

This four-byte field contains the length of this Type-4 record, and specifies the total number of bytes including every byte of every field contained in the record.

5.1.2. Field 4.002: Image Designation Character (IDC)

This is the one-byte binary representation of the IDC number given in the header file.

5.1.3. Field 4.003: Impression Type (IMP)

The impression type is a single-byte field occupying the sixth byte of the record.

Table 4: Finger Impression Type

Code	Description
0	Live-scan of plain fingerprint
1	Live-scan of rolled fingerprint
2	Non-live scan impression of plain fingerprint captured from paper
3	Non-live scan impression of rolled fingerprint captured from paper
4	Latent impression captured directly
5	Latent tracing

Code	Description
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4. Field 4.004: Finger Position (FGP)

This fixed-length field of 6 bytes occupies the seventh through twelfth byte positions of a Type-4 record. It contains possible finger positions beginning in the left most byte (byte 7 of the record). The known or most probable finger position is taken from table 5. Up to five additional fingers may be referenced by entering the alternate finger positions in the remaining five bytes using the same format. If fewer than five finger position references are to be used the unused bytes are filled with binary 255. To reference all finger positions code 0, for unknown, is used.

Table 5: Finger position code and maximum size

Finger position	Finger code	Width (mm)	Length (mm)
Unknown	0	40,0	40,0
Right thumb	1	45,0	40,0
Right index finger	2	40,0	40,0
Right middle finger	3	40,0	40,0
Right ring finger	4	40,0	40,0
Right little finger	5	33,0	40,0
Left thumb	6	45,0	40,0
Left index finger	7	40,0	40,0
Left middle finger	8	40,0	40,0
Left ring finger	9	40,0	40,0
Left little finger	10	33,0	40,0
Plain right thumb	11	30,0	55,0
Plain left thumb	12	30,0	55,0
Plain right four fingers	13	70,0	65,0
Plain left four fingers	14	70,0	65,0

For scene of crime latents only the codes 0 to 10 should be used.

5.1.5. Field 4.005: Image Scanning Resolution (ISR)

This one-byte field occupies the 13th byte of a Type-4 record. If it contains '0' then the image has been sampled at the preferred scanning rate of 19,68 pixels/mm (500 pixels per inch). If it contains '1' then the image has been sampled at an alternative scanning rate as specified in the Type-1 record.

5.1.6. Field 4.006: Horizontal Line Length (HLL)

This field is positioned at bytes 14 and 15 within the Type-4 record. It specifies the number of pixels contained in each scan line. The first byte will be the most significant.

5.1.7. Field 4.007: Vertical Line Length (VLL)

This field records in bytes 16 and 17 the number of scan lines present in the image. The first byte is the most significant.

5.1.8. Field 4.008: Greyscale Compression Algorithm (GCA)

This one-byte field specifies the greyscale compression algorithm used to encode the image data. For this implementation, a binary code 1 indicates that WSQ compression (Appendix 7) has been used.

5.1.9. Field 4.009: The Image

This field contains a byte stream representing the image. Its structure will obviously depend on the compression algorithm used.

6. ***Type-9 Logical Record: Minutiæ Record***

Type-9 records shall contain ASCII text describing minutiæ and related information encoded from a latent. For latent search transaction, there is no limit for these Type-9 records in a file, each of which shall be for a different view or latent.

6.1. *Minutiæ extraction*

6.1.1. Minutia type identification

This standard defines three identifier numbers that are used to describe the minutia type. These are listed in table 6. A ridge ending shall be designated Type 1. A bifurcation shall be designated Type 2. If a minutia cannot be clearly categorised as one of the above two types, it shall be designated as 'other', Type 0.

Table 6: Minutia types

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

6.1.2. Minutia placement and type

For templates to be compliant with Section 5 of the ANSI INCITS 378-2004 standard, the following method, which enhances the current INCITS 378-2004 standard, shall be used for determining placement (location and angular direction) of individual minutiae.

The position or location of a minutia representing a ridge ending shall be the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the three legs of the valley area were thinned down to a single-pixel-wide skeleton, the point of the intersection is the location of the minutia. Similarly, the location of the minutia for a bifurcation shall be the point of forking of the medial skeleton of the ridge. If the three legs of the ridge were each thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia.

After all ridge endings have been converted to bifurcations, all of the minutiae of the dactyloscopic image are represented as bifurcations. The X and Y pixel coordinates of the intersection of the three legs of each minutia can be directly formatted. Determination of the minutia direction can be extracted from each skeleton bifurcation. The three legs of every skeleton bifurcation must be examined and the endpoint of each leg determined. Figure 6.1.2 illustrates the three methods used for determining the end of a leg that is based on a scanning resolution of 500 ppi.

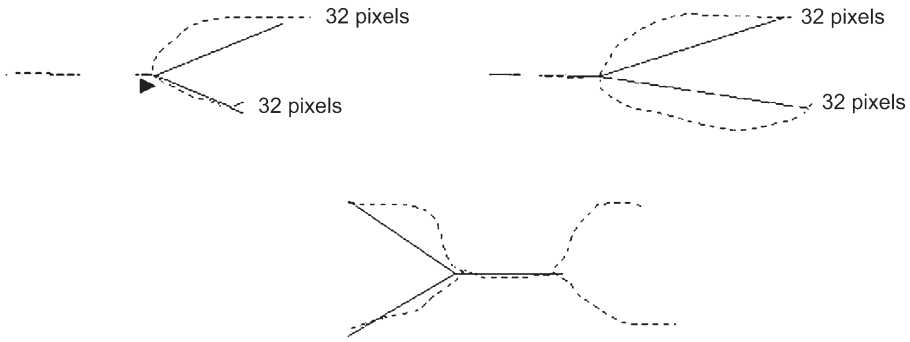
The ending is established according to the event that occurs first. The pixel count is based on a scan resolution of 500 ppi. Different scan resolutions would imply different pixel counts.

— a distance of 0,064" (the 32nd pixel),

— the end of skeleton leg that occurs between a distance of 0,02" and 0,064" (the 10th through the 32nd pixels); shorter legs are not used,

— a second bifurcation is encountered within a distance of 0,064" (before the 32nd pixel).

Figure 6.1.2



The angle of the minutiae is determined by constructing three virtual rays originating at the bifurcation point and extending to the end of each leg. The smallest of the three angles formed by the rays is bisected to indicate the minutiae direction.

6.1.3. Coordinate system

The coordinate system used to express the minutiae of a fingerprint shall be a Cartesian coordinate system. Minutiae locations shall be represented by their x and y coordinates. The origin of the coordinate system shall be the upper left corner of the original image with x increasing to the right and y increasing downward. Both x and y coordinates of a minutiae shall be represented in pixel units from the origin. It should be noted that the location of the origin and units of measure is not in agreement with the convention used in the definitions of the Type 9 in the ANSI/NIST-ITL 1-2000.

6.1.4. Minutiæ direction

Angles are expressed in standard mathematical format, with zero degrees to the right and angles increasing in the counter clockwise direction. Recorded angles are in the direction pointing back along the ridge for a ridge ending and toward the centre of the valley for a bifurcation. This convention is 180 degrees opposite of the angle convention described in the definitions of the Type 9 in the ANSI/NIST-ITL 1-2000.

6.2. *Fields for Type-9 Logical record INCITS-378 Format*

All fields of the Type-9 records shall be recorded as ASCII text. No binary fields are permissible in this tagged-field record.

6.2.1. Field 9.001: Logical record length (LEN)

This mandatory ASCII field shall contain the length of the logical record specifying the total number of bytes, including every character of every field contained in the record.

6.2.2. Field 9.002: Image designation character (IDC)

This mandatory two-byte field shall be used for the identification and location of the minutiæ data. The IDC contained in this field shall match the IDC found in the file content field of the Type-1 record.

6.2.3. Field 9.003: Impression type (IMP)

This mandatory one-byte field shall describe the manner by which the dactyloscopic image information was obtained. The ASCII value of the proper code as selected from table 4 shall be entered in this field to signify the impression type.

6.2.4. Field 9.004: Minutiæ format (FMT)

This field shall contain a 'U' to indicate that the minutiae are formatted in M1-378 terms. Even though information may be encoded in accordance with the M1-378 standard, all data fields of the Type-9 record must remain as ASCII text fields.

6.2.5. Field 9.126: CBEFF information

This field shall contain three information items. The first information item shall contain the value '27' (0x1B). This is the identification of the CBEFF Format Owner assigned by the International Biometric Industry Association (IBIA) to INCITS Technical Committee M1. The <US> character shall delimit this item from the CBEFF Format Type that is assigned a value of '513' (0x0201) to indicate that this record contains only location and angular

direction data without any Extended Data Block information. The <US> character shall delimit this item from the CBEFF Product Identifier (PID) that identifies the 'owner' of the encoding equipment. The vendor establishes this value. It can be obtained from the IBIA website (www.ibia.org) if it is posted.

6.2.6. Field 9.127: Capture equipment identification

This field shall contain two information items separated by the <US> character. The first shall contain 'APPF' if the equipment used originally to acquire the image was certified to comply with Appendix F (IAFIS Image Quality Specification, 29 January 1999) of CJIS-RS-0010, the Federal Bureau of Investigation's Electronic Fingerprint Transmission Specification. If the equipment did not comply it will contain the value of 'NONE'. The second information item shall contain the Capture Equipment ID which is a vendor-assigned product number of the capture equipment. A value of '0' indicates that the capture equipment ID is unreported.

6.2.7. Field 9.128: Horizontal line length (HLL)

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image. The maximum horizontal size is limited to 65 534 pixels.

6.2.8. Field 9.129: Vertical line length (VLL)

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image. The maximum vertical size is limited to 65 534 pixels.

6.2.9. Field 9.130: Scale units (SLC)

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A '1' in this field indicates pixels per inch, or a '2' indicates pixels per centimetre. A '0' in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

6.2.10. Field 9.131: Horizontal pixel scale (HPS)

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a '1' or a '2'. Otherwise, it indicates the horizontal component of the pixel aspect ratio.

6.2.11. Field 9.132: Vertical pixel scale (VPS)

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a '1' or a '2'. Otherwise, it indicates the vertical component of the pixel aspect ratio.

6.2.12. Field 9.133: Finger view

This mandatory field contains the view number of the finger associated with this record's data. The view number begins with '0' and increments by one to '15'.

6.2.13. Field 9.134: Finger position (FGP)

This field shall contain the code designating the finger position that produced the information in this Type-9 record. A code between 1 and 10 taken from table 5 or the appropriate palm code from table 10 shall be used to indicate the finger or palm position.

6.2.14. Field 9.135: Finger quality

The field shall contain the quality of the overall finger minutiæ data and shall be between 0 and 100. This number is an overall expression of the quality of the finger record, and represents quality of the original image, of the minutia extraction and any additional operations that may affect the minutiæ record.

6.2.15. Field 9.136: number of minutiæ

The mandatory field shall contain a count of the number of minutiæ recorded in this logical record.

6.2.16. Field 9.137: Finger minutiæ data

This mandatory field has six information items separated by the <US> character. It consists of several subfields, each containing the details of single minutiae. The total number of minutiae subfields must agree with the count found in field 136. The first information item is the minutiae index number, which shall be initialised to '1' and incremented by '1' for each additional minutia in the fingerprint. The second and third information items are the 'x' coordinate and 'y' coordinates of the minutiae in pixel units. The fourth information item is the minutiae angle recorded in units of two degrees. This value shall be nonnegative between 0 and 179. The fifth information item is the minutiae type. A value of '0' is used to represent minutiae of type 'OTHER', a value of '1' for a ridge ending and a value of '2' for a ridge bifurcation. The sixth information item represents the quality of each minutiae. This value shall range from 1 as a minimum to 100 as a maximum. A value of '0' indicates that no quality value is available. Each subfield shall be separated from the next with the use of the <RS> separator character.

6.2.17. Field 9.138: Ridge count information

This field consists of a series of subfields each containing three information items. The first information item of the first subfield shall indicate the ridge count extraction method. A '0' indicates that no assumption shall be made about the method used to extract ridge counts, nor their order in the record. A '1' indicates that for each centre minutiae, ridge count data was extracted to the nearest neighbouring minutiae in four quadrants, and ridge counts for each centre minutia are listed together. A '2' indicates that for each centre minutiae, ridge count data was extracted to the nearest neighbouring minutiae in eight octants, and ridge counts for each centre minutia are listed together. The remaining two information items of the first subfield shall both contain '0'. Information items shall be separated by the <US> separator character. Subsequent subfields will contain the centre minutiae index number as the first information item, the neighbouring minutiae index number as the second information item, and the number of ridges crossed as the third information item. Subfields shall be separated by the <RS> separator character.

6.2.18. Field 9.139: Core information

This field will consist of one subfield for each core present in the original image. Each subfield consists of three information items. The first two items contain the 'x' and 'y' coordinate positions in pixel units. The third information item contains the angle of the core recorded in units of 2 degrees. The value shall be a nonnegative value between 0 and 179. Multiple cores will be separated by the <RS> separator character.

6.2.19. Field 9.140: Delta information

This field will consist of one subfield for each delta present in the original image. Each subfield consists of three information items. The first two items contain the 'x' and 'y' coordinate positions in pixel units. The third information item contains the angle of the delta recorded in units of 2 degrees. The value shall be a nonnegative value between 0 and 179. Multiple cores will be separated by the <RS> separator character.

7. ***Type-13 variable-resolution latent image record***

The Type-13 tagged-field logical record shall contain image data acquired from latent images. These images are intended to be transmitted to agencies that will automatically extract or provide human intervention and processing to extract the desired feature information from the images.

Information regarding the scanning resolution used, the image size, and other parameters required to process the image, are recorded as tagged-fields within the record.

Table 7: Type-13 variable-resolution latent record layout

Ident	Cond. code	Field Number	Field name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	13.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	13.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	13.003	IMPRESSION TYPE	A	2	2	1	1	9
SRC	M	13.004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
LCD	M	13.005	LATENT CAPTURE DATE	N	9	9	1	1	16

Ident	Cond. code	Field Number	Field name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
HLL	M	13.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	13.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	13.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	13.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	13.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	13.011	COMPRESSION ALGORITHM	A	5	7	1	1	14
BPX	M	13.012	BITS PER PIXEL	N	2	3	1	1	10
FGP	M	13.013	FINGER POSITION	N	2	3	1	6	25
RSV		13.014 13.019	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
COM	O	13.020	COMMENT	A	2	128	0	1	135
RSV		13.021 13.199	RESERVED FOR FUTURE DEFINITION	—	—	—	—	—	—
UDF	O	13.200 13.998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	13.999	IMAGE DATA	B	2	—	1	1	—

Key for character type: N = Numeric; A = Alphabetic; AN = Alphanumeric; B = Binary

7.1. *Fields for the Type-13 logical record*

The following paragraphs describe the data contained in each of the fields for the Type-13 logical record.

Within a Type-13 logical record, entries shall be provided in numbered fields. It is required that the first two fields of the record are ordered, and the field containing the image data shall be the last physical field in the record. For each field of the Type-13 record, table 7 lists the 'condition code' as being mandatory 'M' or optional 'O', the field number, the field name, character type, field size, and occurrence limits. Based on a three digit field number, the maximum byte count size for the field is given in the last column. As more digits are used for the field number, the maximum byte count will also increase. The two entries in the 'field size per occurrence' include all character separators used in the field. The 'maximum byte count' includes the field number, the information, and all the character separators including the 'GS' character.

7.1.1. Field 13.001: Logical record length (LEN)

This mandatory ASCII field shall contain the total count of the number of bytes in the Type-13 logical record. Field 13.001 shall specify the length of the record including every character of every field contained in the record and the information separators.

7.1.2. Field 13.002: Image designation character (IDC)

This mandatory ASCII field shall be used to identify the latent image data contained in the record. This IDC shall match the IDC found in the file content (CNT) field of the Type-1 record.

7.1.3. Field 13.003: Impression type (IMP)

This mandatory one- or two-byte ASCII field shall indicate the manner by which the latent image information was obtained. The appropriate latent code choice selected from table 4 (finger) or table 9 (palm) shall be entered in this field.

7.1.4. Field 13.004: Source agency/ORI (SRC)

This mandatory ASCII field shall contain the identification of the administration or organisation that originally captured the facial image contained in the record. Normally, the Originating Agency Identifier (ORI) of the agency that captured the image will be contained in this field. It consists of two information items in the following format: CC/agency.

The first information item contains the Interpol Country Code, two alpha-numeric characters long. The second item, agency, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

7.1.5. Field 13.005: Latent capture date (LCD)

This mandatory ASCII field shall contain the date that the latent image contained in the record was captured. The date shall appear as eight digits in the format CCYYMMDD. The CCYY characters shall represent the year the image was captured; the MM characters shall be the tens and unit values of the month; and the DD characters shall be the tens and unit values of the day in the month. For example, 20000229 represents 29 February 2000. The complete date must be a legitimate date.

7.1.6. Field 13.006: Horizontal line length (HLL)

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image.

7.1.7. Field 13.007: Vertical line length (VLL)

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image.

7.1.8. Field 13.008: Scale units (SLC)

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A '1' in this field indicates pixels per inch, or a '2' indicates pixels per centimetre. A '0' in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

7.1.9. Field 13.009: Horizontal pixel scale (HPS)

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a '1' or a '2'. Otherwise, it indicates the horizontal component of the pixel aspect ratio.

7.1.10. Field 13.010: Vertical pixel scale (VPS)

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a '1' or a '2'. Otherwise, it indicates the vertical component of the pixel aspect ratio.

7.1.11. Field 13.011: Compression algorithm (CGA)

This mandatory ASCII field shall specify the algorithm used to compress greyscale images. See Appendix 7 for the compression codes.

7.1.12. Field 13.012: Bits per pixel (BPX)

This mandatory ASCII field shall contain the number of bits used to represent a pixel. This field shall contain an entry of '8' for normal greyscale values of '0' to '255'. Any entry in this field greater than '8' shall represent a greyscale pixel with increased precision.

7.1.13. Field 13.013: Finger/palm position (FGP)

This mandatory tagged-field shall contain one or more the possible finger or palm positions that may match the latent image. The decimal code number corresponding to the known or most probable finger position shall be taken from table 5 or the most probable palm position from table 10 and entered as a one- or two-character ASCII subfield. Additional finger and/or palm positions may be referenced by entering the alternate position codes as subfields separated by the 'RS' separator character. The code '0', for 'Unknown Finger', shall be used to reference every finger position from one through ten. The code '20', for 'Unknown Palm', shall be used to reference every listed palmprint position.

7.1.14. Field 13.014-019: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

7.1.15. Field 13.020: Comment (COM)

This optional field may be used to insert comments or other ASCII text information with the latent image data.

7.1.16. Field 13.021-199: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

7.1.17. Fields 13.200-998: User-defined fields (UDF)

These fields are user-definable fields and will be used for future requirements. Their size and content shall be defined by the user and be in accordance with the receiving agency. If present they shall contain ASCII textual information.

7.1.18. Field 13.999: Image data (DAT)

This field shall contain all data from a captured latent image. It shall always be assigned field number 999 and must be the last physical field in the record. For example, '13.999*:*' is followed by image data in a binary representation.

Each pixel of uncompressed greyscale data shall normally be quantised to eight bits (256 grey levels) contained in a single byte. If the entry in BPX Field 13.012 is greater or less than '8', the number of bytes required to contain a pixel will be different. If compression is used, the pixel data shall be compressed in accordance with the compression technique specified in the GCA field.

7.2. *End of Type-13 variable-resolution latent image record*

For the sake of consistency, immediately following the last byte of data from Field 13.999 an 'FS' separator shall be used to separate it from the next logical record. This separator must be included in the length field of the Type-13 record.

8. ***Type-15 variable-resolution palmprint image record***

The Type-15 tagged-field logical record shall contain and be used to exchange palmprint image data together with fixed and user-defined textual information fields pertinent to the digitised image. Information regarding the scanning resolution used, the image size and other parameters or comments required to process the image are recorded as tagged-fields within the record. Palmprint images transmitted to other agencies will be processed by the recipient agencies to extract the desired feature information required for matching purposes.

The image data shall be acquired directly from a subject using a live-scan device, or from a palmprint card or other media that contains the subject's palmprints.

Any method used to acquire the palmprint images shall be capable of capturing a set of images for each hand. This set shall include the writer's palm as a single scanned image, and the entire area of the full palm extending from the wrist bracelet to the tips of the fingers as one or two scanned images. If two images are used to represent the full palm, the lower image shall extend from the wrist bracelet to the top of the interdigital area (third finger joint) and shall include the thenar, and hypothenar areas of the palm. The upper image shall extend from the bottom of the interdigital area to the upper tips of the fingers. This provides an adequate amount of overlap between the two images that are both located over the interdigital area of the palm. By matching the ridge structure and details contained in this common area, an examiner can confidently state that both images came from the same palm.

As a palmprint transaction may be used for different purposes, it may contain one or more unique image areas recorded from the palm or hand. A complete palmprint record set for one individual will normally include the writer's palm and the full palm image(s) from each hand. Since a tagged-field logical image record may contain only one binary field, a single Type-15 record will be required for each writer's palm and one or two Type-15 records for each full palm. Therefore, four to six Type-15 records will be required to represent the subject's palmprints in a normal palmprint transaction.

8.1. *Fields for the Type-15 logical record*

The following paragraphs describe the data contained in each of the fields for the Type-15 logical record.

Within a Type-15 logical record, entries shall be provided in numbered fields. It is required that the first two fields of the record are ordered, and the field containing the image data shall be the last physical field in the record. For each field of the Type-15 record, table 8 lists the 'condition code' as being mandatory 'M' or optional 'O', the field number, the field name, character type, field size, and occurrence limits. Based on a three digit field number, the maximum byte count size for the field is given in the last column. As more digits are used for the field number, the maximum byte count will also increase. The two entries in the 'field size per occurrence' include all character separators used in the field. The 'maximum byte count' includes the field number, the information, and all the character separators including the 'GS' character.

8.1.1. Field 15.001: Logical record length (LEN)

This mandatory ASCII field shall contain the total count of the number of bytes in the Type-15 logical record. Field 15.001 shall specify the length of the record including every character of every field contained in the record and the information separators.

8.1.2. Field 15.002: Image designation character (IDC)

This mandatory ASCII field shall be used to identify the palmprint image contained in the record. This IDC shall match the IDC found in the file content (CNT) field of the Type-1 record.

8.1.3. Field 15.003: Impression type (IMP)

This mandatory one-byte ASCII field shall indicate the manner by which the palmprint image information was obtained. The appropriate code selected from table 9 shall be entered in this field.

8.1.4. Field 15.004: Source agency/ORI (SRC)

This mandatory ASCII field shall contain the identification of the administration or organisation that originally captured the facial image contained in the record. Normally, the Originating Agency Identifier (ORI) of the agency that captured the image will be contained in this field. It consists of two information items in the following format: CC/agency.

The first information item contains the Interpol Country Code, two alpha-numeric characters long. The second item, agency, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

8.1.5. Field 15.005: Palmprint capture date (PCD)

This mandatory ASCII field shall contain the date that the palmprint image was captured. The date shall appear as eight digits in the format CCYYMMDD. The CCYY characters shall represent the year the image was captured; the MM characters shall be the tens and unit values of the month; and the DD characters shall be the tens and units values of the day in the month. For example, the entry 20000229 represents 29 February 2000. The complete date must be a legitimate date.

8.1.6. Field 15.006: Horizontal line length (HLL)

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image.

8.1.7. Field 15.007: Vertical line length (VLL)

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image.

8.1.8. Field 15.008: Scale units (SLC)

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A '1' in this field indicates pixels per inch, or a '2' indicates pixels per centimetre. A '0' in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

8.1.9. Field 15.009: Horizontal pixel scale (HPS)

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a '1' or a '2'. Other-wise, it indicates the horizontal component of the pixel aspect ratio.

8.1.10. Field 15.010: Vertical pixel scale (VPS)

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a '1' or a '2'. Otherwise, it indicates the vertical component of the pixel aspect ratio.

Table 8: Type-15 variable-resolution palmprint record layout

Ident	Cond. code	Field number	Field name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	15.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	15.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	15.003	IMPRESSION TYPE	N	2	2	1	1	9
SRC	M	15.004	SOURCE AGENCY/ORI	AN	6	35	1	1	42
PCD	M	15.005	PALMPRINT CAPTURE DATE	N	9	9	1	1	16
HLL	M	15.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	15.011	COMPRESSION ALGORITHM	AN	5	7	1	1	14
BPX	M	15.012	BITS PER PIXEL	N	2	3	1	1	10
PLP	M	15.013	PALMPRINT POSITION	N	2	3	1	1	10
RSV		15.014 15.019	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
COM	O	15.020	COMMENT	AN	2	128	0	1	128
RSV		15.021 15.199	RESERVED FOR FUTURE INCLUSION	—	—	—	—	—	—
UDF	O	15.200 15.998	USER-DEFINED FIELDS	—	—	—	—	—	—
DAT	M	15.999	IMAGE DATA	B	2	—	1	1	—

Table 9: Palm Impression Type

Description	Code
Live-scan palm	10
Nonlive-scan palm	11
Latent palm impression	12
Latent palm tracing	13
Latent palm photo	14
Latent palm lift	15

8.1.11. Field 15.011: Compression algorithm (CGA)

This mandatory ASCII field shall specify the algorithm used to compress greyscale images. An entry of 'NONE' in this field indicates that the data contained in this record are uncompressed. For those images that are to be compressed, this field shall contain the preferred method for the compression of tenprint fingerprint images. Valid compression codes are defined in Appendix 7.

8.1.12. Field 15.012: Bits per pixel (BPX)

This mandatory ASCII field shall contain the number of bits used to represent a pixel. This field shall contain an entry of '8' for normal greyscale values of '0' to '255'. Any entry in this field greater than or less than '8' shall represent a greyscale pixel with increased or decreased precision respectively.

Table 10: Palm Codes, Areas and Sizes

Palm Position	Palm code	Image area (mm^2)	Width (mm)	Height (mm)
Unknown Palm	20	28 387	139,7	203,2
Right Full Palm	21	28 387	139,7	203,2
Right Writer s Palm	22	5 645	44,5	127,0
Left Full Palm	23	28 387	139,7	203,2
Left Writer s Palm	24	5 645	44,5	127,0
Right Lower Palm	25	19 516	139,7	139,7
Right Upper Palm	26	19 516	139,7	139,7
Left Lower Palm	27	19 516	139,7	139,7
Left Upper Palm	28	19 516	139,7	139,7
Right Other	29	28 387	139,7	203,2
Left Other	30	28 387	139,7	203,2

8.1.13. Field 15.013: Palmprint position (PLP)

This mandatory tagged-field shall contain the palmprint position that matches the palmprint image. The decimal code number corresponding to the known or most probable palmprint position shall be taken from table 10 and entered as a two-character ASCII subfield. Table 10 also lists the maximum image areas and dimensions for each of the possible palmprint positions.

8.1.14. Field 15.014-019: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

8.1.15. Field 15.020: Comment (COM)

This optional field may be used to insert comments or other ASCII text information with the palmprint image data.

8.1.16. Field 15.021-199: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

8.1.17. Fields 15.200-998: User-defined fields (UDF)

These fields are user-definable fields and will be used for future requirements. Their size and content shall be defined by the user and be in accordance with the receiving agency. If present they shall contain ASCII textual information.

8.1.18. Field 15.999: Image data (DAT)

This field shall contain all of the data from a captured palmprint image. It shall always be assigned field number 999 and must be the last physical field in the record. For example, '15.999:' is followed by image data in a binary representation. Each pixel of uncompressed greyscale data shall normally be quantised to eight bits (256 grey levels) contained in a single byte. If the entry in BPX Field 15.012 is greater or less than 8, the number of bytes required to contain a pixel will be different. If compression is used, the pixel data shall be compressed in accordance with the compression technique specified in the CGA field.

8.2. *End of Type-15 variable-resolution palmprint image record*

For the sake of consistency, immediately following the last byte of data from Field 15.999 an 'FS' separator shall be used to separate it from the next logical record. This separator must be included in the length field of the Type-15 record.

8.3. *Additional Type-15 variable-resolution palmprint image records*

Additional Type-15 records may be included in the file. For each additional palmprint image, a complete Type-15 logical record together with the 'FS' separator is required.

Table 11: Maximum numbers of candidates accepted for verification per transmission

Type of AFIS Search	TP/TP	LT/TP	LP/PP	TP/UL	LT/UL	PP/ULP	LP/ULP
Maximum Number of Candidates	1	10	5	5	5	5	5

Search types:

TP/TP: ten-print against ten-print

LT/TP: fingerprint latent against ten-print

LP/PP: palmprint latent against palmprint

TP/UL: ten-print against unsolved fingerprint latent

LT/UL: fingerprint latent against unsolved fingerprint latent

PP/ULP: palmprint against unsolved palmprint latent

LP/ULP: palmprint latent against unsolved palmprint latent

9. ***Appendices to Chapter 2 (exchange of dactyloscopic data)***

9.1. *Appendix 1 ASCII Separator Codes*

ASCII	Position ([1])	Description
LF	1/10	Separates error codes in Field 2.074
FS	1/12	Separates logical records of a file
GS	1/13	Separates fields of a logical record
RS	1/14	Separates the subfields of a record field
US	1/15	Separates individual information items of the field or subfield

([1]) This is the position as defined in the ASCII standard.

9.2. *Appendix 2 Calculation of Alpha-Numeric Check Character*

For TCN and TCR (Fields 1.09 and 1.10):

The number corresponding to the check character is generated using the following formula:

(YY * 10^{8} + SSSSSSSS) Modulo 23

Where YY and SSSSSSSS are the numerical values of the last two digits of the year and the serial number respectively.

The check character is then generated from the look-up table given below.

For CRO (Field 2.010)

The number corresponding to the check character is generated using the following formula:

(YY * 10^6 + NNNNNN) Modulo 23

Where YY and NNNNNN are the numerical values of the last two digits of the year and the serial number respectively.

The check character is then generated from the look-up table given below.

Check Character Look-up Table

1-A	9-J	17-T
2-B	10-K	18-U
3-C	11-L	19-V
4-D	12-M	20-W
5-E	13-N	21-X
6-F	14-P	22-Y
7-G	15-Q	0-Z
8-H	16-R	

9.3. *Appendix 3 Character Codes*

7-bit ANSI code for information interchange

ASCII Character Set

+	0	1	2	3	4	5	6	7	8	9
30				!	’	#	$	%	&	‘
40	(	)	*	+	,	-	.	/	0	1
50	2	3	4	5	6	7	8	9	:	;
60	<	=	>	?	@	A	B	C	D	E
70	F	G	H	I	J	K	L	M	N	O
80	P	Q	R	S	T	U	V	W	X	Y
90	Z	[	\	]	^	_	`	a	b	c
100	d	e	f	g	h	i	j	k	l	m
110	n	o	p	q	r	s	t	u	v	w
120	x	y	z	{	|	}	~			

9.4. *Appendix 4 Transaction Summary*

Type 1 Record (mandatory)

Identifier	Field number	Field name	CPS/PMS	SRE	ERR
LEN	1.001	Logical Record Length	M	M	M
VER	1.002	Version Number	M	M	M
CNT	1.003	File Content	M	M	M

Identifier	Field number	Field name	CPS/PMS	SRE	ERR
TOT	1.004	Type of Transaction	M	M	M
DAT	1.005	Date	M	M	M
PRY	1.006	Priority	M	M	M
DAI	1.007	Destination Agency	M	M	M
ORI	1.008	Originating Agency	M	M	M
TCN	1.009	Transaction Control Number	M	M	M
TCR	1.010	Transaction Control Reference	C	M	M
NSR	1.011	Native Scanning Resolution	M	M	M
NTR	1.012	Nominal Transmitting Resolution	M	M	M
DOM	1.013	Domain name	M	M	M
GMT	1.014	Greenwich mean time	M	M	M

Under the Condition Column:

O = Optional; M = Mandatory; C = Conditional if transaction is a response to the origin agency

Type 2 Record (mandatory)

Identifier	Field number	Field name	CPS/ PMS	MPS/ MMS	SRE	ERR
LEN	2.001	Logical Record Length	M	M	M	M
IDC	2.002	Image Designation Character	M	M	M	M
SYS	2.003	System Information	M	M	M	M
CNO	2.007	Case Number	—	M	C	—
SQN	2.008	Sequence Number	—	C	C	—
MID	2.009	Latent Identifier	—	C	C	—
CRN	2.010	Criminal Reference Number	M	—	C	—
MN1	2.012	Miscellaneous Identification Number	—	—	C	C
MN2	2.013	Miscellaneous Identification Number	—	—	C	C
MN3	2.014	Miscellaneous Identification Number	—	—	C	C
MN4	2.015	Miscellaneous Identification Number	—	—	C	C
INF	2.063	Additional Information	O	O	O	O
RLS	2.064	Respondents List	—	—	M	—
ERM	2.074	Status/Error Message Field	—	—	—	M
ENC	2.320	Expected Number of Candidates	M	M	—	—

Under the Condition Column:

O = Optional; M = Mandatory; C = Conditional if data is available

* = if the transmission of the data is in accordance with national law (not covered by the Council Decision 2008/615/JHA)

9.5. *Appendix 5 Type-1 Record Definitions*

Identifier	Condition	Field number	Field name	Character type	Example data
LEN	M	1.001	Logical Record Length	N	1.001:230{GS}
VER	M	1.002	Version Number	N	1.002:0300{GS}
CNT	M	1.003	File Content	N	1.003:1{US}15{RS}2{US}00{RS}4{US}01{RS}4{US}02{RS}4{US}03{RS}4{US}04{RS}4{US}05{RS}4{US}06{RS}4{US}07{RS}4{US}08{RS}4{US}09{RS}4{US}10{RS}4{US}11{RS}4{US}12{RS}4{US}13{RS}4{US}14{GS}
TOT	M	1.004	Type of Transaction	A	1.004:CPS{GS}
DAT	M	1.005	Date	N	1.005:20050101{GS}
PRY	M	1.006	Priority	N	1.006:4{GS}
DAI	M	1.007	Destination Agency	1*	1.007:DE/BKA{GS}
ORI	M	1.008	Originating Agency	1*	1.008:NL/NAFIS{GS}
TCN	M	1.009	Transaction Control Number	AN	1.009:0200000004F{GS}
TCR	C	1.010	Transaction Control Reference	AN	1.010:0200000004F{GS}
NSR	M	1.011	Native Scanning Resolution	AN	1.011:19.68{GS}
NTR	M	1.012	Nominal Transmitting Resolution	AN	1.012:19,68{GS}
DOM	M	1.013	Domain Name	AN	1.013: INT-I{US}4,22{GS}
GMT	M	1.014	Greenwich Mean Time	AN	1.014:20050101125959Z

Under the Condition Column: O = Optional, M = Mandatory, C = Conditional

Under the Character Type Column: A = Alpha, N = Numeric, B = Binary

1* allowed characters for agency name are ['0..9', 'A..Z', 'a..z', '_', '.', ' ', '-']

9.6. *Appendix 6 Type-2 Record Definitions*

Table A.6.1: CPS- and PMS-Transaction

Identifier	Condition	Field number	Field name	Character type	Example data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	M	2.010	Criminal Reference Number	AN	2.010:DE/E999999999{GS}

Identifier	Condition	Field number	Field name	Character type	Example data
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Table A.6.2: SRE-Transaction

Identifier	Condition	Field number	Field name	Character type	Example data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	C	2.010	Criminal Reference Number	AN	2.010:NL/2222222222{GS}
MN1	C	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
RLS	M	2.064	Respondents List	AN	2.064:CPS{RS}I{RS}001/001{RS}999999{GS}

Table A.6.3: ERR-Transaction

Identifier	Condition	Field number	Field name	Character type	Example data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
MN1	M	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}

Identifier	Condition	Field number	Field name	Character type	Example data
ERM	M	2.074	Status/Error Message Field	AN	2.074: 201: IDC - 1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION {GS}

Table A.6.4: MPS- and MMS-Transaction

Identifier	Condition	Field number	Field name	Character type	Example data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CNO	M	2.007	Case Number	AN	2.007:E999999999{GS}
SQN	C	2.008	Sequence Number	N	2.008:0001{GS}
MID	C	2.009	Latent Identifier	A	2.009:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123 {GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Under the Condition Column: O = Optional, M = Mandatory, C = Conditional

Under the Character Type Column: A = Alpha, N = Numeric, B = Binary

1* allowed characters are ['0..9', 'A..Z', 'a..z', '_', '.', ' ', '-',',']

9.7. *Appendix 7 Greyscale Compression Codes*

Compression Codes

Compression	Value	Remarks
Wavelet Scalar Quantisation Greyscale Fingerprint Image Compression Specification IAFIS-IC-0010(V3), dated 19 December 1997	WSQ	Algorithm to be used for the compression of greyscale images in Type-4, Type-7 and Type-13 to Type-15 records. Shall not be used for resolutions > 500dpi.
JPEG 2000 [ISO 15444/ITU T.800]	J2K	To be used for lossy and losslessly compression of greyscale images in Type-13 to Type-15 records. Strongly recommended for resolutions > 500 dpi

9.8. *Appendix 8 Mailspecification*

To improve the internal workflow the mailsubject of a PRUEM transaction has to be filled with the country code (CC) of the Member State that send the message and the Type of Transaction (TOT Field 1.004).

Format: CC/type of transaction

Example: 'DE/CPS'

The mailbody can be empty.

CHAPTER 3: **Exchange of vehicle registration data**

1. ***Common data-set for automated search of vehicle registration data***

1.1. *Definitions*

The definitions of mandatory data elements and optional data elements set out in Article 16(4) are as follows:

Mandatory (M):

The data element has to be communicated when the information is available in a Member State's national register. Therefore there is an obligation to exchange the information when available.

Optional (O):

The data element may be communicated when the information is available in a Member State's national register. Therefore there is no obligation to exchange the information even when the information is available.

An indication (Y) is given for each element in the data set where the element is specifically identified as important in relation with the Decision 2008/615/JHA.

1.2. *Vehicle/owner/holder search*

1.2.1. Triggers for the search

There are two different ways to search for the information as defined in the next paragraph:

— by Chassis Number (VIN), Reference Date and Time (optional),

— by License Plate Number, Chassis Number (VIN) (optional), Reference Date and Time (optional).

By means of these search criteria, information related to one and sometimes more vehicles will be returned. If information for only one vehicle has to be returned, all the items are returned in one response. If more than one vehicle is found, the requested Member State itself can determine which items will be returned; all items or only the items to refine the search (e.g. because of privacy reasons or because of performance reasons).

The items necessary to refine the search are pictured in paragraph 1.2.2.1. In paragraph 1.2.2.2 the complete information set is described.

When the search is done by Chassis Number, Reference Date and Time, the search can be done in one or all of the participating Member States.

When the search is done by License Number, Reference Data and Time, the search has to be done in one specific Member State.

Normally the actual Date and Time is used to make a search, but it is possible to conduct a search with a Reference Date and Time in the past. When a search is made with a Reference Date and Time in the past and historical information is not available in the register of the specific Member State because no such information is registered at all, the actual information can be returned with an indication that the information is actual information.

1.2.2. Data set

1.2.2.1. Items to be returned necessary for the refinement of the search

Item	M/O [1]	Remarks	Prüm Y/N [2]
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1 [3]) e.g. Ford, Opel, Renault, etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	Y

Item	M/O (1)	Remarks	Prüm Y/N (2)
EU Category Code	M	(J) mopeds, motorbikes, cars, etc.	Y

(1) M = mandatory when available in national register, O = optional.
(2) All the attributes specifically allocated by the Member States are indicated with Y.
(3) Harmonised document abbreviation, see Council Directive 1999/37/EC of 29 April 1999.

1.2.2.2. Complete data set

Item	M/O (1)	Remarks	Prüm Y/N
Data relating to holders of the vehicle		(C.1 (2)) The data refer to the holder of the specific registration certificate.	
Registration holders' (company) name	M	(C.1.1.) separate fields will be used for surname, infixes, titles, etc., and the name in printable format will be communicated	Y
First name	M	(C.1.2) separate fields for first name(s) and initials will be used, and the name in printable format will be communicated	Y
Address	M	(C.1.3) separate fields will be used for Street, House number and Annex, Zip code, Place of residence, Country of residence, etc., and the Address in printable format will be communicated	Y
Gender	M	Male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm, etc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date holdership	O	Start date of the holdership of the car. This date will often be the same as printed under (I) on the registration certificate of the vehicle.	N
End date holdership	O	End data of the holdership of the car.	N
Type of holder	O	If there is no owner of the vehicle (C.2) the reference to the fact that the holder of the registration certificate: — is the vehicle owner, — is not the vehicle owner, — is not identified by the registration certificate as being the vehicle owner.	N
Data relating to owners of the vehicle		(C.2)	
Owners' (company) name	M	(C.2.1)	Y
First name	M	(C.2.2)	Y

Item	M/O [1]	Remarks	Prüm Y/N
Address	M	(C.2.3)	Y
Gender	M	male, female	Y
Date of birth	M		Y
Legal entity	M	individual, association, company, firm, etc.	Y
Place of Birth	O		Y
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date ownership	O	Start date of the ownership of the car.	N
End date ownership	O	End data of the ownership of the car.	N
Data relating to vehicles			
Licence number	M		Y
Chassis number/VIN	M		Y
Country of registration	M		Y
Make	M	(D.1) e.g. Ford, Opel, Renault, etc.	Y
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane.	Y
Nature of the vehicle/EU Category Code	M	(J) mopeds, motorbikes, cars, etc.	Y
Date of first registration	M	(B) Date of first registration of the vehicle somewhere in the world.	Y
Start date (actual) registration	M	(I) Date of the registration to which the specific certificate of the vehicle refers.	Y
End date registration	M	End data of the registration to which the specific certificate of the vehicle refers. It is possible this date indicates the period of validity as printed on the document if not unlimited (document abbreviation = H).	Y
Status	M	Scrapped, stolen, exported, etc.	Y
Start date status	M		Y
End date status	O		N
kW	O	(P.2)	Y
Capacity	O	(P.1)	Y
Type of licence number	O	Regular, transito, etc.	Y
Vehicle document id 1	O	The first unique document ID as printed on the vehicle document.	Y
Vehicle document id 2 [3]	O	A second document ID as printed on the vehicle document.	Y
Data relating to insurances			
Insurance company name	O		Y
Begin date insurance	O		Y
End date insurance	O		Y
Address	O		Y
Insurance number	O		Y

Item	M/O (1)	Remarks	Prüm Y/N
ID number	O	An identifier that uniquely identifies the company.	N
Type of ID number	O	The type of ID number (e.g. number of the Chamber of Commerce)	N

(1) M = mandatory when available in national register, O = optional.
(2) Harmonised document abbreviation, see Council Directive 1999/37/EC of 29 April 1999.
(3) In Luxembourg two separate vehicle registration document ID's are used.

2. ***Data Security***

2.1. *Overview*

The Eucaris software application handles secure communication to the other Member States and communicates to the back-end legacy systems of Member States using XML. Member States exchange messages by directly sending them to the recipient. The data centre of a Member State is connected to the TESTA network of EU.

The XML-messages sent over the network are encrypted. The technique to encrypt these messages is SSL. The messages sent to the back-end are plain text XML-messages since the connection between the application and the back-end shall be in a protected environment.

A client application is provided which can be used within a Member State to query their own register or other Member States' registers. The clients will be identified by means of user-id/password or a client certificate. The connection to a user may be encrypted, but this is the responsibility of each individual Member State.

2.2. *Security Features related to message exchange*

The security design is based on a combination of HTTPS and XML signature. This alternative uses XML-signature to sign all messages sent so the server and can authenticate the sender of the message by checking the signature. 1-sided SSL (only a server certificate) is used to protect the confidentiality and integrity of the message in transit and provides protection against deletion/replay and insertion attacks. Instead of bespoke software development to implement 2-sided SSL, XML-signature is implemented. Using XML-signature is closer to the web services roadmap than 2-sided SSL and therefore more strategic.

The XML-signature can be implemented in several ways but the chosen approach is to use XML Signature as part of the Web Services Security (WSS). WSS specifies how to use XML-signature. Since WSS builds upon the SOAP standard, it is logical to adhere to the SOAP standard as much as possible.

2.3. *Security features not related to message exchange*

2.3.1. Authentication of users

The users of the Eucaris web application authenticate themselves using a username and password. Since standard Windows authentication is used, Member States can enhance the level of authentication of users if needed by using client certificates.

2.3.2. User roles

The Eucaris software application supports different user roles. Each cluster of services has its own authorisation. E.g. (exclusive) users of the '"Treaty of Eucaris" — functionality' may not use the '"Prüm" — functionality'. Administrator services are separated from the regular end-user roles.

2.3.3. Logging and tracing of message exchange

Logging of all message types is facilitated by the Eucaris software application. An administrator function allows the national administrator to determine which messages are logged: requests from end-users, incoming requests from other Member States, provided information from the national registers, etc.

The application can be configured to use an internal database for this logging, or an external (Oracle) database. The decision on what messages have to be logged clearly depends on logging facilities elsewhere in the legacy systems and connected client applications.

The header of each message contains information on the requesting Member State, the requesting organisation within that Member State and the user involved. Also the reason of the request is indicated.

By means of the combined logging in the requesting and responding Member State complete tracing of any message exchange is possible (e.g. on request of a citizen involved).

Logging is configured through the Eucaris web client (menu Administration, Logging configuration). The logging functionality is performed by the Core System. When logging is enabled, the complete message (header and body) is stored in one logging record. Per defined service, and per message type that passes along the Core System, the logging level can be set.

Logging Levels

The following logging levels are possible:

Private — Message is logged: The logging is NOT available to the extract logging service but is available on a national level only, for audits and problem solving.

None — Message is not logged at all.

Message Types

Information exchange between Member States consists of several messages, of which a schematic representation is given in the figure below.

The possible message types (in the figure shown for the Eucaris Core System of Member State X) are the following:

1. Request to Core System_Request message by Client
2. Request to Other Member State_Request message by Core System of this Member State
3. Request to Core System of this Member State_Request message by Core System of other Member State
4. Request to Legacy Register_Request message by Core System
5. Request to Core System_Request message by Legacy Register
6. Response from Core System_Request message by Client
7. Response from Other Member State_Request message by Core System of this Member State
8. Response from Core System of this Member State_Request message by other Member State
9. Response from Legacy Register_Request message by Core System
10. Response from Core System_Request message by Legacy Register

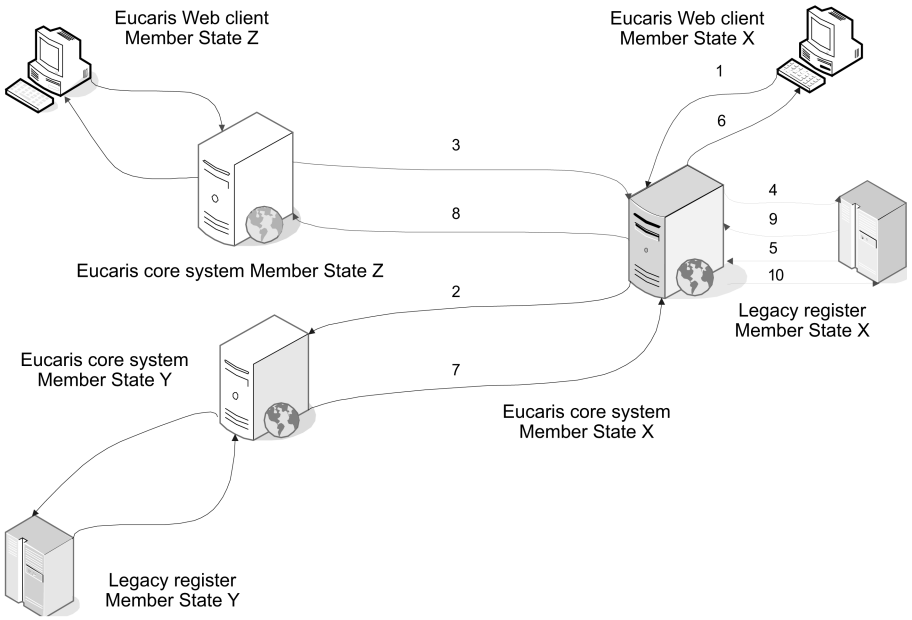
The following information exchanges are shown in the figure:

— Information request from Member State X to Member State Y — blue arrows. This request and response consists of message types 1, 2, 7 and 6, respectively,

— Information request from Member State Z to Member State X — red arrows. This request and response consists of message types 3, 4, 9 and 8, respectively,

— Information request from the legacy register to its core system (this route also includes a request from a custom client behind the legacy register) — green arrows. This kind of request consists of message types 5 and 10,

Figure: Message types for logging



2.3.4. Hardware Security Module

A Hardware Security Module is not used.

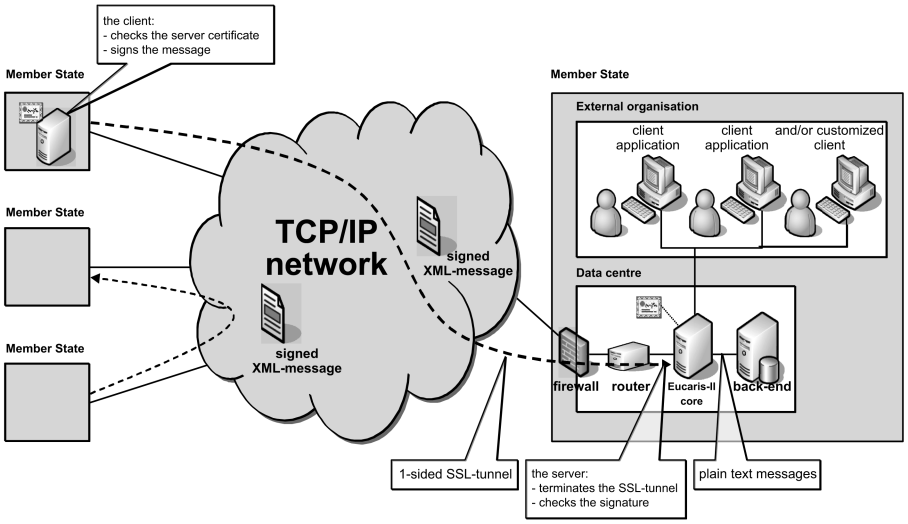
A Hardware Security Module (HSM) provides good protection for the key used to sign messages and to identify servers. This adds to the overall level of security but an HSM is expensive to buy/maintain and there are no requirements to decide for a FIPS 140-2 level 2 or level 3 HSM. Since a closed network is used that mitigates threats effectively, it is decided not to use an HSM initially. If an HSM is necessary e.g. to obtain accreditation, it can be added to the architecture.

3. *Technical conditions of the data exchange*

3.1. *General description of the Eucaris application*

3.1.1. Overview

The Eucaris application connects all participating Member States in a mesh network where each Member State communicates directly to another Member State. There is no central component needed for the communication to be established. The Eucaris application handles secure communication to the other Member States and communicates to the back-end legacy systems of Member States using XML. The following picture visualises this architecture.



Member State exchange messages by directly sending them to the recipient. The data centre of a Member State is connected to the network used for the message exchange (TESTA). To access the TESTA network, Member States connect to TESTA via their national gate. A firewall shall be used to connect to the network and a router connects the Eucaris application to the firewall. Depending on the alternative chosen to protect the messages, a certificate is used either by the router or by the Eucaris application.

A client application is provided which can be used within a Member State to query its own register or other Member States' registers. The client application connects to Eucaris. The clients will be identified by means of user-id/password or a client certificate. The connection to a user in an external organisation (e.g. police) may be encrypted but this is the responsibility of each individual Member State.

3.1.2. Scope of the system

The scope of the Eucaris system is limited to the processes involved in the exchange of information between the Registration Authorities in the Member States and a basic presentation of this information. Procedures and automated processes in which the information is to be used, are outside the scope of the system.

Member States can choose either to use the Eucaris client functionality or to set up their own customised client application. In the table below, it is described which aspects of the Eucaris system are mandatory to use and/or prescribed and which are optional to use and/or free to determine by the Member States.

Eucaris aspects	M/O [1]	Remark
Network concept	M	The concept is an 'any-to-any' communication.
Physical network	M	TESTA
Core application	M	The core application of Eucaris has to be used to connect to the other Member States. The following functionality is offered by the core: — Encrypting and signing of the messages; — Checking of the identity of the sender; — Authorisation of Member States and local users; — Routing of messages; — Queuing of asynchronous messages if the recipient service is temporally unavailable; — Multiple country inquiry functionality; — Logging of the exchange of messages; — Storage of incoming messages
Client application	O	In addition to the core application the Eucaris II client application can be used by a Member State. When applicable, the core and client application are modified under auspices of the Eucaris organisation.
Security concept	M	The concept is based on XML-signing by means of client certificates and SSL-encryption by means of service certificates.
Message specifications	M	Every Member State has to comply with the message specifications as set by the Eucaris organisation and this Council Decision. The specifications can only be changed by the Eucaris organisation in consultation with the Member States.
Operation and Support	M	The acceptance of new Member States or a new functionality is under auspices of the Eucaris organisation. Monitoring and help desk functions are managed centrally by an appointed Member State.

[1] M = mandatory to use or to comply with O = optional to use or to comply with.

3.2. *Functional and Non Functional Requirements*

3.2.1. Generic functionality

In this section the main generic functions have been described in general terms.

No	Description
1.	The system allows the Registration Authorities of the Member States to exchange request and response messages in an interactive way.
2.	The system contains a client application, enabling end-users to send their requests and presenting the response information for manual processing
3.	The system facilitates 'broadcasting', allowing a Member State to send a request to all other Member States. The incoming responses are consolidated by the core application in one response message to the client application (this functionality is called a 'Multiple Country Inquiry).
4.	The system is able to deal with different types of messages. User roles, authorisation, routing, signing and logging are all defined per specific service.
5.	The system allows the Member States to exchange batches of messages or messages containing a large number of requests or replies. These messages are dealt with in an asynchronous way.
6.	The system queues asynchronous messages if the recipient Member State is temporarily unavailable and guarantees the deliverance as soon as the recipient is up again.
7.	The system stores incoming asynchronous messages until they can be processed.
8.	The system only gives access to Eucaris applications of other Member States, not to individual organisations within those other Member States, i.e. each Registration Authority acts as the single gateway between its national end-users and the corresponding Authorities in the other Member States.
9.	It is possible to define users of different Member States on one Eucaris server and to authorise them following the rights of that Member State.
10.	Information on the requesting Member State, organisation and end user are included in the messages.
11.	The system facilitates logging of the exchange of messages between the different Member States and between the core application and the national registration systems.
12.	The system allows a specific secretary, which is an organisation or Member State explicitly appointed for this task, to gather logged information on messages sent/received by all the participating Member States, in order to produce statistical reports.
13.	Each Member State indicates itself what logged information is made available for the secretary and what information is 'private'.
14.	The system allows the National Administrators of each Member State to extract statistics of use.
15.	The system enables addition of new Member States through simple administrative tasks.

3.2.2. Usability

No	Description
16.	The system provides an interface for automated processing of messages by back-end systems/legacy and enables the integration of the user interface in those systems (customised user-interface).
17.	The system is easy to learn, self explanatory and contains help-text.
18.	The system is documented to assist Member States in integration, operational activities and future maintenance (e.g. reference guides, functional/technical documentation, operational guide, …).
19.	The user interface is multi-lingual and offers facilities for the end-user to select a preferred language.
20.	The user interface contains facilities for a Local Administrator to translate both screen-items and coded information to the national language.

3.2.3. Reliability

No	Description
21.	The system is designed as a robust and dependable operational system which is tolerant to operator errors and which will recover cleanly from power cuts or other disasters. It must be possible to restart the system with no or minimal loss of data.
22.	The system must give stable and reproducible results.
23.	The system has been designed to function reliably. It is possible to implement the system in a configuration that guarantees an availability of 98 % (by redundancy, the use of back-up servers, etc.) in each bilateral communication.
24.	It is possible to use part of the system, even during failure of some components (if Member State C is down, Member States A and B are still able to communicate). The number of single points of failure in the information chain should be minimised.
25.	The recovery time after a severe failure should be less than one day. It should be possible to minimise down-time by using remote support, e.g. by a central service desk.

3.2.4. Performance

No	Description
26.	The system can be used 24x7. This time-window (24x7) is then also required from the Member States' legacy systems.
27.	The system responds rapidly to user requests irrespective of any background tasks. This is also required from the Parties legacy systems to ensure acceptable response time. An overall response time of 10 seconds maximum for a single request is acceptable.
28.	The system has been designed as a multi-user system and in such a way that background tasks can continue while the user performs foreground tasks.
29.	The system has been designed to be scaleable in order to support the potential increase of number of messages when new functionality is added or new organisations or Member States are added.

3.2.5. Security

No	Description
30.	The system is suited (e.g. in its security measures) for the exchange of messages containing privacy-sensitive personal data (e.g. car owner/holders), classified as EU restricted.
31.	The system is maintained in such a way that unauthorised access to the data is prevented.
32.	The system contains a service for the management of the rights and permissions of national end-users.
33.	Member States are able to check the identity of the sender (at Member State level), by means of XML-signing.
34.	Member States must explicitly authorise other Member States to request specific information.
35.	The system provides at application level a full security and encryption policy compatible with the level of security required in such situations. Exclusiveness and integrity of the information is guaranteed by the use of XML-signing and encryption by means of SSL-tunnelling.
36.	All exchange of messages can be traced by means of logging.
37.	Protection is provided against deletion attacks (a third party deletes a message) and replay or insertion attacks (a third party replays or inserts a message).
38.	The system makes use of certificates of a Trusted Third Party (TTP).
39.	The system is able to handle different certificates per Member State, depending on the type of message or service.

No	Description
40.	The security measures at application level are sufficient to allow the use of non accredited networks.
41.	The system is able to use novice security techniques such as an XML-firewall.

3.2.6. Adaptability

No	Description
42.	The system is extensible with new messages and new functionality. The costs of adaptations are minimal. Due to the centralised development of application components.
43.	Member States are able to define new message types for bilateral use. Not all Member States are required to support all message types.

3.2.7. Support and Maintenance

No	Description
44.	The system provides monitoring facilities for a central service-desk and/or operators concerning the network and servers in the different Member States.
45.	The system provides facilities for remote support by a central service-desk.
46.	The system provides facilities for problem analysis.
47.	The system can be expanded to new Member States.
48.	The application can easily be installed by staff with a minimum of IT-qualifications and experience. The installation procedure shall be as much as possible automated.
49.	The system provides a permanent testing and acceptance environment.
50.	The annual costs of maintenance and support has been minimised by adherence to market standards and by creating the application in such a way that as little support as possible from a central service-desk is required.

3.2.8. Design requirements

No	Description
51.	The system is designed and documented for an operational lifetime of many years.
52.	The system has been designed in such a way that it is independent of the network provider.
53.	The system is compliant with the existing HW/SW in the Member States by interacting with those registration systems using open standard web service technology (XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509, etc.).

3.2.9. Applicable standards

No	Description
54.	The system is compliant with data protection issues as stated in Regulation EC 45/2001 (Articles 21, 22 and 23) and Directive 95/46/EC.
55.	The system complies with the IDA Standards.
56.	The system supports UTF8.

CHAPTER 4: **Evaluation**

1. ***Evaluation procedure according to Article 20 (Preparation of decisions according to Article 25(2) of decision 2008/615/JHA)***

1.1. *Questionnaire*

The relevant Council Working Group shall draw up a questionnaire concerning each of the automated data exchanges set out in Chapter 2 of Decision 2008/615/JHA.

As soon as a Member State believes it fulfils the prerequisites for sharing data in the relevant data category, it shall answer the relevant questionnaire.

1.2. *Pilot run*

With a view to evaluating the results of the questionnaire, the Member State that wishes to start sharing data shall carry out a pilot run together with one or more other Member States already sharing data under the Council Decision. The pilot run takes place shortly before or shortly after the evaluation visit.

The conditions and arrangements for this pilot run will be identified by the relevant Council Working Group and be based upon prior individual agreement with the concerned Member State. The Member States taking part in the pilot run will decide on the practical details.

1.3. *Evaluation visit*

With a view to evaluating the results of the questionnaire, an evaluation visit shall take place in the Member State that wishes to start sharing data.

The conditions and arrangement for this visit will be identified by the relevant Working Group and be based upon prior individual agreement between the concerned Member State and the evaluation team. The concerned Member State will enable the evaluation team to check the automated exchange of data in the data category or categories to be evaluated, in particular by organising a programme for the visit which takes into account the requests of the evaluation team.

Within one month, the evaluation team will produce a report on the evaluation visit and will forward it to the Member State concerned for its comments. If appropriate, this report will be revised by the evaluation team on the basis of the Member State's comments.

The evaluation team will consist of no more than three experts, designated by the Member States taking part in the automated data exchange in the data categories to be evaluated, who have experience regarding the concerned data category, have the appropriate national security clearance to deal with these matters and are willing to take part in at least one evaluation visit in another Member State. The Commission will be invited to join the evaluation team as observer.

The members of the evaluation team will respect the confidential nature of the information they acquire when carrying out their task.

1.4. *Report to the Council*

An overall evaluation report, summarising the results of the questionnaires, the evaluation visit and the pilot run, will be presented to the Council for its decision pursuant to Article 25(2) of Decision 2008/615/JHA.

2. ***Evaluation procedure according to Article 21***

2.1. *Statistics and report*

Each Member State will compile statistics on the results of the automated data exchange. In order to ensure comparability, the model for statistics will be compiled by the relevant Council Working Group.

These statistics will be forwarded annually to the General Secretariat, which will produce a summary overview for the elapsed year, and to the Commission.

In addition, Member States will be requested on a regular basis not to exceed once per year to provide further information on the administrative, technical and financial implementation of automated data exchange as needed to analyse and improve the process. On the basis of this information, a report will be produced for the Council.

2.2. *Revision*

Within reasonable time, the Council will examine the evaluation mechanism described here and revise it as necessary.

3. Expert meetings

Within the relevant Council Working Group, experts will meet regularly to organise and implement the abovementioned evaluation procedures as well as to share experience and discuss possible improvements. Where applicable, the results of these expert discussions will be incorporated into the report referred to in 2.1.

III

(Acts adopted under the EU Treaty)

ACTS ADOPTED UNDER TITLE VI OF THE EU TREATY

COUNCIL FRAMEWORK DECISION 2009/905/JHA

of 30 November 2009

on Accreditation of forensic service providers carrying out laboratory activities

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 30(1)(a) and (c) and Article 34(2)(b) thereof,

Having regard to the initiative of the Kingdom of Sweden and the Kingdom of Spain [1],

Having regard to the opinion of the European Parliament,

Whereas:

(1) The European Union has set itself the objective of maintaining and developing the Union as an area of freedom, security and justice; a high level of safety is to be provided by common action among the Member States in the field of police and judicial cooperation in criminal matters.

(2) That objective is to be achieved by preventing and combating crime through closer cooperation between law enforcement authorities in the Member States, while respecting the principles and rules relating to human rights, fundamental freedoms and the rule of law on which the Union is founded and which are common to the Member States.

(3) Exchange of information and intelligence on crime and criminal activities is crucial for the possibility for law enforcement authorities to successfully prevent, detect and investigate crime or criminal activities. Common action in the field of police cooperation under Article 30(1)(a) of the Treaty entails the need to process relevant information which should be subject to appropriate provisions on the protection of personal data.

(4) The intensified exchange of information regarding forensic evidence and the increased use of evidence from one Member State in the judicial processes of another, highlights the need to establish common standards for forensic service providers.

(5) Information originating from forensic processes in one Member State may currently be associated with a level of uncertainty in another Member State regarding the way in which an item has been handled, what methods have been used and how the results have been interpreted.

(6) In point 3.4 (h) of the Council and Commission Action Plan implementing The Hague Programme on strengthening freedom, security and justice in the European Union [2] Member States stressed the need for a definition of the quality standards of forensic laboratories by 2008.

(7) It is particularly important to introduce common standards for forensic service providers relating to such sensitive personal data as DNA profiles and dactyloscopic data.

(8) Pursuant to Article 7(4) of Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [3], Member States shall take the necessary measures to guarantee the integrity of DNA profiles made available or sent for comparison to other Member States and to ensure that these measures comply with international standards, such as EN ISO/IEC 17025 'General requirements for the competence of testing and calibration laboratories' (hereinafter 'EN ISO/IEC 17025').

[1] OJ C 174, 28.7.2009, p. 7.

[2] OJ C 198, 12.8.2005, p. 1.

[3] OJ L 210, 6.8.2008, p. 12.

(9) DNA profiles and dactyloscopic data are not only used in criminal proceedings but are also crucial for the identification of victims, particularly after disasters.

(10) The accreditation of forensic service providers carrying out laboratory activities is an important step towards a safer and more effective exchange of forensic information within the Union.

(11) Accreditation is granted by the national accreditation body which has exclusive competence to assess if a laboratory meets the requirements set by harmonised standards. An accreditation body derives its authority from the State. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products [1] contains detailed provisions on the competence of such national accreditation bodies. Inter alia, Article 7 of that Regulation regulates cross-border accreditation in cases where accreditation may be requested from another national accreditation body.

(12) The absence of an agreement to apply a common accreditation standard for the analysis of scientific evidence is a deficiency that should be remedied; it is, therefore, necessary to adopt a legally binding instrument on the accreditation of all forensic service providers carrying out laboratory activities. Accreditation offers the necessary guarantees that laboratory activities are performed in accordance with relevant international standards, in particular EN ISO/IEC 17025, as well as relevant applicable guidelines.

(13) An accreditation standard allows any Member State to require, if it wishes, complementary standards in laboratory activities within its national jurisdiction.

(14) Accreditation will help establish mutual trust in the validity of the basic analytic methods used. However, accreditation does not state which method to use, only that the method used has to be suitable for its purpose.

(15) Any measure taken outside a laboratory is beyond the scope of this Framework Decision. For example, the taking of dactyloscopic data or measures taken at the scene of incident, the scene of crime or forensic analyses carried out outside laboratories are not included in its scope.

(16) This Framework Decision does not aim to harmonise national rules regarding the judicial assessment of forensic evidence.

(17) This Decision does not affect the validity, established in accordance with national applicable rules, of the results of laboratory activities carried out prior to its implementation, even if the forensic service provider was not accredited to comply with EN ISO/IEC 17025,

HAS ADOPTED THIS FRAMEWORK DECISION:

Article 1

Objective

1. The purpose of this Framework Decision is to ensure that the results of laboratory activities carried out by accredited forensic service providers in one Member State are recognised by the authorities responsible for the prevention, detection and investigation of criminal offences as being equally reliable as the results of laboratory activities carried out by forensic service providers accredited to EN ISO/IEC 17025 within any other Member State.

2. This purpose is achieved by ensuring that forensic service providers carrying out laboratory activities are accredited by a national accreditation body as complying with EN ISO/IEC 17025.

Article 2

Scope

This Framework Decision shall apply to laboratory activities resulting in:

(a) DNA-profile; and

(b) dactyloscopic data.

Article 3

Definitions

For the purposes of this Framework Decision:

(a) 'laboratory activity' means any measure taken in a laboratory when locating and recovering traces on items, as well as developing, analysing and interpreting forensic evidence, with a view to providing expert opinions or exchanging forensic evidence;

(b) 'results of laboratory activities' means any analytical outputs and directly associated interpretation;

(c) 'forensic service provider' means any organisation, public or private, that carries out forensic laboratory activities at the request of competent law enforcement or judicial authorities;

[1] OJ L 218, 13.8.2008, p. 30.

(d) 'national accreditation body' means the sole body in a Member State that performs accreditation with authority derived from the State as referred to in Regulation (EC) No 765/2008;

(e) 'DNA-profile' means a letter or number code which represents a set of identification characteristics of the non-coding part of an analysed human DNA sample, i.e. the particular molecular structure at the various DNA locations (loci);

(f) 'dactyloscopic data' means fingerprint images, images of fingerprint latents, palm prints, palm print latents and templates of such images (coded minutiae).

Article 4

Accreditation

Member States shall ensure that their forensic service providers carrying out laboratory activities are accredited by a national accreditation body as complying with EN ISO/IEC 17025.

Article 5

Recognition of results

1. Each Member State shall ensure that the results of accredited forensic service providers carrying out laboratory activities in other Member States are recognised by its authorities responsible for the prevention, detection, and investigation of criminal offences as being equally reliable as the results of domestic forensic service providers carrying out laboratory activities accredited to EN ISO/IEC 17025.

2. This Framework Decision does not affect national rules on the judicial assessment of evidence.

Article 6

Costs

1. Each Member State shall bear any public costs resulting from this Framework Decision in accordance with national arrangements.

2. The Commission shall examine the means to provide financial support from the general budget of the European Union for national and transnational projects intended to contribute to the implementation of this Framework Decision, inter alia for the exchange of experience, dissemination of know-how and proficiency testing.

Article 7

Implementation

1. Member States shall take the necessary steps to comply with the provisions of this Framework Decision in relation to DNA-profiles by 30 November 2013.

2. Member States shall take the necessary steps to comply with the provisions of this Framework Decision in relation to dactyloscopic data by 30 November 2015.

3. Member States shall forward to the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national laws the obligations imposed on them under this Framework Decision by 30 May 2016 at the latest.

4. On the basis of the information referred to in paragraph 3 and other information provided by the Member States on request, the Commission shall, before 1 July 2018, submit a report to the Council on the implementation and application of this Framework Decision.

5. The Council shall, by the end of 2018, assess the extent to which Member States have complied with this Framework Decision.

Article 8

Entry into force

This Framework Decision shall enter into force on the twentieth day following its publication in the *Official Journal of the European Union*.

Done at Brussels, 30 November 2009.

For the Council
The President
B. ASK

DECISIONS

COUNCIL DECISION

of 27 November 2014

determining certain consequential and transitional arrangements concerning the cessation of the participation of the United Kingdom of Great Britain and Northern Ireland in certain acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon

(2014/836/EU)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to Protocol No 36 on transitional provisions (hereinafter 'Protocol No 36'), annexed to the Treaty on European Union, to the Treaty on the Functioning of the European Union and to the Treaty establishing the European Atomic Energy Community, and in particular the second subparagraph of Article 10(4) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) Under Protocol No 36, the United Kingdom had the possibility to notify to the Council, by 31 May 2014, that it does not accept the powers of the Commission and of the Court of Justice, introduced by the Treaty of Lisbon, with respect to acts of the Union in the field of police cooperation and judicial cooperation in criminal matters which had been adopted before the entry into force of the Treaty of Lisbon.

(2) By letter to the President of the Council dated 24 July 2013, the United Kingdom notified the Council that it does not accept the powers of the Commission and of the Court of Justice introduced by the Treaty of Lisbon in the field of police cooperation and judicial cooperation in criminal matters. As a consequence, the relevant acts in the field of police cooperation and judicial cooperation in criminal matters cease to apply to the United Kingdom on 1 December 2014.

(3) The United Kingdom may notify its wish to participate in the acts which have ceased to apply to it.

(4) The United Kingdom has indicated its intention to notify its wish to participate in some of those acts.

(5) In accordance with the second subparagraph of Article 10(4) of Protocol No 36, the Council should, on a proposal from the Commission, determine the necessary consequential and transitional arrangements. The Council may also, on the basis of the third subparagraph of Article 10(4), determine that the United Kingdom should bear the direct financial consequences necessarily and unavoidably incurred as a result of the cessation of its participation in those acts.

(6) Any disruption in the implementation and application of the acts which the United Kingdom has sought to rejoin should be avoided. Those acts should therefore continue to apply to the United Kingdom for a limited transitional period until the decisions of the Council and the Commission authorising the participation of the United Kingdom take effect.

(7) As the United Kingdom has not notified the Council of its wish to participate in Council Decisions 2008/615/JHA ([1]) and 2008/616/JHA ([2]) and Council Framework Decision 2009/905/JHA ([3]) (hereinafter 'the Prüm Decisions'), they will cease to apply to the United Kingdom as from 1 December 2014. As a consequence

([1]) Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).
([2]) Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).
([3]) Council Framework Decision 2009/905/JHA of 30 November 2009 on accreditation of forensic service providers carrying out laboratory activities (OJ L 322, 9.12.2009, p. 14).

of the cessation of their application, and until such time as the United Kingdom rejoins the Prüm Decisions, it should be prevented from accessing for law enforcement purposes the Eurodac database set up under Regulation (EU) No 603/2013 of the European Parliament and of the Council ([1]).

(8) However, given the practical and operational significance of the Prüm Decisions to the Union for public security, and more particularly for law enforcement and the prevention, detection and investigation of criminal offences, the United Kingdom should, in close consultation with operational partners in the United Kingdom, the Member States, the Commission, Europol and Eurojust, undertake a full business and implementation case in order to assess the merits and practical benefits of the United Kingdom rejoining the Prüm Decisions and the necessary steps for it to do so, the results of which should be published by 30 September 2015.

(9) If the above business and implementation case is positive, the United Kingdom should decide, by 31 December 2015, on whether to notify the Council, within the following four weeks, of its wish to participate in the Prüm Decisions, in accordance with Article 10(5) of Protocol No 36. The United Kingdom has indicated that a positive vote in its Parliament is required before such decision is taken.

(10) The rules on the financial consequences incurred as a result of the cessation of the participation of the United Kingdom in the Prüm Decisions will be provided for in Council Decision 2014/837/EU ([2]).

(11) In accordance with the second subparagraph of Article 10(4) of Protocol No 36, the United Kingdom is not participating in the adoption of this Decision, but is bound by it,

HAS ADOPTED THIS DECISION:

Article 1

The acts which are listed in the Annex shall continue to apply to the United Kingdom until 7 December 2014.

Article 2

1. Within 10 days of 30 November 2014, the United Kingdom shall begin to undertake a full business and implementation case in order to assess the merits and practical benefits of the United Kingdom rejoining the Prüm Decisions and the necessary steps for it to do so.

It shall do so in close consultation with operational partners in the United Kingdom, the Member States, the Commission, Europol and Eurojust.

2. By 30 September 2015, the United Kingdom shall publish the results of the business and implementation case referred to in paragraph 1.

3. If the business and implementation case is positive, the United Kingdom shall decide by 31 December 2015 whether to notify the Council of its wish to participate in the Prüm Decisions in accordance with Article 10(5) of Protocol No 36. The notification shall be made within four weeks from 31 December 2015.

([1]) Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (OJ L 180, 29.6.2013, p. 1).

([2]) Council Decision 2014/837/EU of 27 November 2014 determining certain direct financial consequences incurred as a result of the cessation of the participation of the United Kingdom of Great Britain and Northern Ireland in certain acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon (see page 17 of this Official Journal).

Article 3

Until such time as a decision confirming the United Kingdom's participation in the Prüm Decisions takes effect, the United Kingdom shall be prevented from accessing for law enforcement purposes the Eurodac database set up under Regulation (EU) No 603/2013.

Article 4

If the United Kingdom has not notified the Council of its wish to participate in the Prüm Decisions within four weeks from 31 December 2015, the Commission shall submit a report to the European Parliament and to the Council on the effects of the non-participation of the United Kingdom in those Decisions.

Article 5

This Decision shall enter into force on 30 November 2014.

Done at Brussels, 27 November 2014.

For the Council
The President
A. GIACOMELLI

ANNEX

LIST OF ACTS REFERRED TO IN ARTICLE 1

1. Convention implementing the Schengen Agreement of 1985: Article 39, Article 40, Articles 42 and 43 (to the extent that they relate to Article 40), Article 44, Article 46, Article 47 (except paragraphs (2)(c) and (4)), Articles 54 to 58, Article 59, Articles 61 to 69, Article 71, Article 72, Articles 126 to 130 (to the extent that they relate to the provisions of the Schengen Convention in which the United Kingdom participates), and Final Act — Declaration No 3 (concerning Article 71(2)) (OJ L 239, 22.9.2000, p. 19)

2. Council Decision 2000/586/JHA of 28 September 2000 establishing a procedure for amending Articles 40(4) and (5), 41(7) and 65(2) of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders (OJ L 248, 3.10.2000, p. 1)

3. Council Decision 2003/725/JHA of 2 October 2003 amending the provisions of Article 40(1) and (7) of the Convention implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders (OJ L 260, 11.10.2003, p. 37)

4. Joint Action 97/827/JHA of 5 December 1997 establishing a mechanism for evaluating the application and implementation at national level of international undertakings in the fight against organized crime (OJ L 344, 15.12.1997, p. 7)

5. Council Act of 18 December 1997 drawing up, on the basis of Article K.3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations (OJ C 24, 23.1.1998, p. 1)

6. Joint Action 98/700/JHA of 3 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union concerning the setting up of a European Image Archiving System (FADO) (OJ L 333, 9.12.1998, p. 4)

7. Council Decision 2000/375/JHA of 29 May 2000 to combat child pornography on the internet (OJ L 138, 9.6.2000, p. 1)

8. Council Decision 2000/641/JHA of 17 October 2000 establishing a secretariat for the joint supervisory data-protection bodies set up by the Convention on the establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention) (OJ L 271, 24.10.2000, p. 1)

9. Council Decision 2000/642/JHA of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information (OJ L 271, 24.10.2000, p. 4)

10. Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002, p. 1)

11. Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 245, 29.9.2003, p. 44)

12. Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 138, 4.6.2009, p. 14)

13. Council Decision 2002/348/JHA of 25 April 2002 concerning security in connection with football matches with an international dimension (OJ L 121, 8.5.2002, p. 1)

14. Council Decision 2007/412/JHA of 12 June 2007 amending Decision 2002/348/JHA concerning security in connection with football matches with an international dimension (OJ L 155, 15.6.2007, p. 76)

15. Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams (OJ L 162, 20.6.2002, p. 1)

16. Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1)

    17. Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial (OJ L 81, 27.3.2009, p. 24)

18. Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties (OJ L 76, 22.3.2005, p. 16)

    — Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial (OJ L 81, 27.3.2009, p. 24)

19. Council Framework Decision 2006/783/JHA of 6 October 2006 on the application of the principle of mutual recognitions to confiscation orders (OJ L 328, 24.11.2006, p. 59)

    — Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial (OJ L 81, 27.3.2009, p. 24)

20. Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386, 29.12.2006, p. 89)

21. Commission Decision 2007/171/EC of 16 March 2007 laying down the network requirements for the Schengen Information System II (third pillar) (OJ L 79, 20.3.2007, p. 29)

22. Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63)

23. Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or property related to, crime (OJ L 332, 18.12.2007, p. 103)

24. Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60)

25. Council Framework Decision 2008/675/JHA of 24 July 2008 on taking account of convictions in the Member States of the European Union in the course of new criminal proceedings (OJ L 220, 15.8.2008, p. 32)

26. Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purposes of their enforcement in the European Union (OJ L 327, 5.12.2008, p. 27)

    — Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial (OJ L 81, 27.3.2009, p. 24)

27. Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network (OJ L 348, 24.12.2008, p. 130)

28. Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23)

    29. Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA (OJ L 93, 7.4.2009, p. 33)

30. Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37)

31. Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information (OJ L 325, 11.12.2009, p. 6)

32. Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files (OJ L 325, 11.12.2009, p. 14)

33. Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information (OJ L 332, 17.12.2009, p. 17)

34. Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention (OJ L 294, 11.11.2009, p. 20)

35. Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes (OJ L 323, 10.12.2009, p. 20)

COUNCIL DECISION

of 27 November 2014

determining certain direct financial consequences incurred as a result of the cessation of the participation of the United Kingdom of Great Britain and Northern Ireland in certain acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon

(2014/837/EU)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to Protocol No 36 on transitional provisions (hereinafter 'Protocol No 36'), annexed to the Treaty on European Union, to the Treaty on the Functioning of the European Union and to the Treaty establishing the European Atomic Energy Community, and in particular the third subparagraph of Article 10(4) thereof,

Having regard to the proposal from the European Commission,

Whereas:

(1) Under Protocol No 36, the United Kingdom had the possiblity to notify to the Council, by 31 May 2014, that it does not accept the powers of the Commission and of the Court of Justice, introduced by the Treaty of Lisbon, with respect to acts of the Union in the field of police cooperation and judicial cooperation in criminal matters which had been adopted before the entry into force of the Treaty of Lisbon.

(2) By letter to the President of the Council dated 24 July 2013, the United Kingdom notified the Council that it does not accept the powers of the Commission and of the Court of Justice introduced by the Treaty of Lisbon in the field of police cooperation and judicial cooperation in criminal matters. As a consequence, the relevant acts in the field of police cooperation and judicial cooperation in criminal matters cease to apply to the United Kingdom on 1 December 2014.

(3) The United Kingdom may notify its wish to participate in the acts which have ceased to apply to it.

(4) The United Kingdom has indicated its intention to notify its wish to participate in some of those acts.

(5) In accordance with the second subparagraph of Article 10(4) of Protocol No 36, the Council should, on a proposal from the Commission, determine the necessary consequential and transitional arrangements. The Council may also, on the basis of the third subparagraph of Article 10(4), determine that the United Kingdom should bear the direct financial consequences necessarily and unavoidably incurred as a result of the cessation of its participation in those acts.

(6) As the United Kingdom has not notified the Council of its wish to participate in Council Decisions 2008/615/JHA ([1]) and 2008/616/JHA ([2]) and Council Framework Decision 2009/905/JHA ([3]) (hereinafter 'the Prüm Decisions'), they will cease to apply to the United Kingdom as from 1 December 2014. However, given the practical and operational significance of the Prüm Decisions to the Union for public security, and more particularly for law enforcement and the prevention, detection and investigation of criminal offences, the Council

([1]) Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 1).
([2]) Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (OJ L 210, 6.8.2008, p. 12).
([3]) Council Framework Decision 2009/905/JHA of 30 November 2009 on accreditation of forensic service providers carrying out laboratory activities (OJ L 322, 9.12.2009, p. 14).

decided by Decision 2014/836/EU [1] that the United Kingdom is to undertake a full business and implementation case in order to assess the merits and practical benefits of the United Kingdom rejoining the Prüm Decisions and the necessary steps for it to do so, the results of which are to be published by 30 September 2015. If the business and implementation case is positive, the United Kingdom will decide, by 31 December 2015, whether to notify the Council, within the following four weeks, of its wish to participate in the Prüm Decisions, in accordance with Article 10(5) of Protocol No 36.

(7) Funds from the Programme 'Prevention of and Fight against Crime', established by Council Decision 2007/125/JHA [2], have been allocated to the United Kingdom for two projects related to Decisions 2008/615/JHA and 2008/616/JHA, first concerning the implementation by the United Kingdom of the Prüm DNA Exchange, with a maximum co-funding of EUR 961 019 granted to the Home Office, and second concerning the Prüm Fingerprint Evaluation by the United Kingdom, with a maximum co-funding of EUR 547 836 granted to the Home Office. This amounts to a total of EUR 1 508 855.

(8) In case the United Kingdom does not respect one of the deadlines set out in Article 2 of Decision 2014/836/EU, or decides not to participate in the Prüm Decisions, it should repay, as a direct financial consequence necessarily and unavoidably incurred as a result of the cessation of its participation in the Prüm Decisions, the sums actually paid by the Commission as a contribution from the general budget of the Union for the implementation of those Decisions.

(9) In accordance with the third subparagraph of Article 10(4) of Protocol No 36, the United Kingdom is participating in the adoption of this Decision and is bound by it,

HAS ADOPTED THIS DECISION:

Article 1

In case the United Kingdom does not respect one of the deadlines set out in Article 2 of Decision 2014/836/EU, or decides not to participate in the Prüm Decisions, it shall repay to the general budget of the Union the sums, up to EUR 1 508 855, received under the Programme 'Prevention of and Fight against Crime'.

Article 2

This Decision shall enter into force on 1 December 2014.

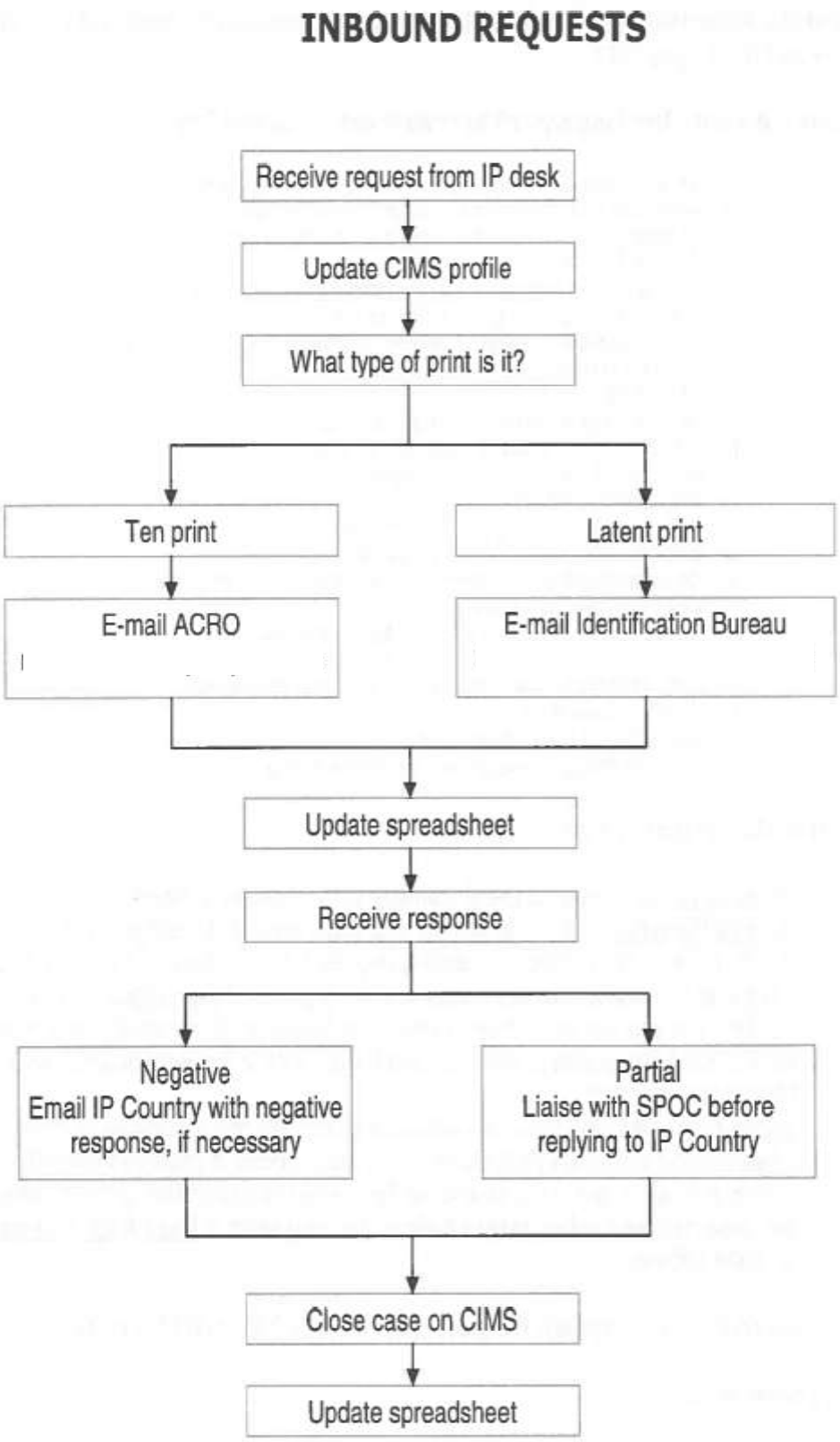
Done at Brussels, 27 November 2014.

For the Council
The President
A. GIACOMELLI

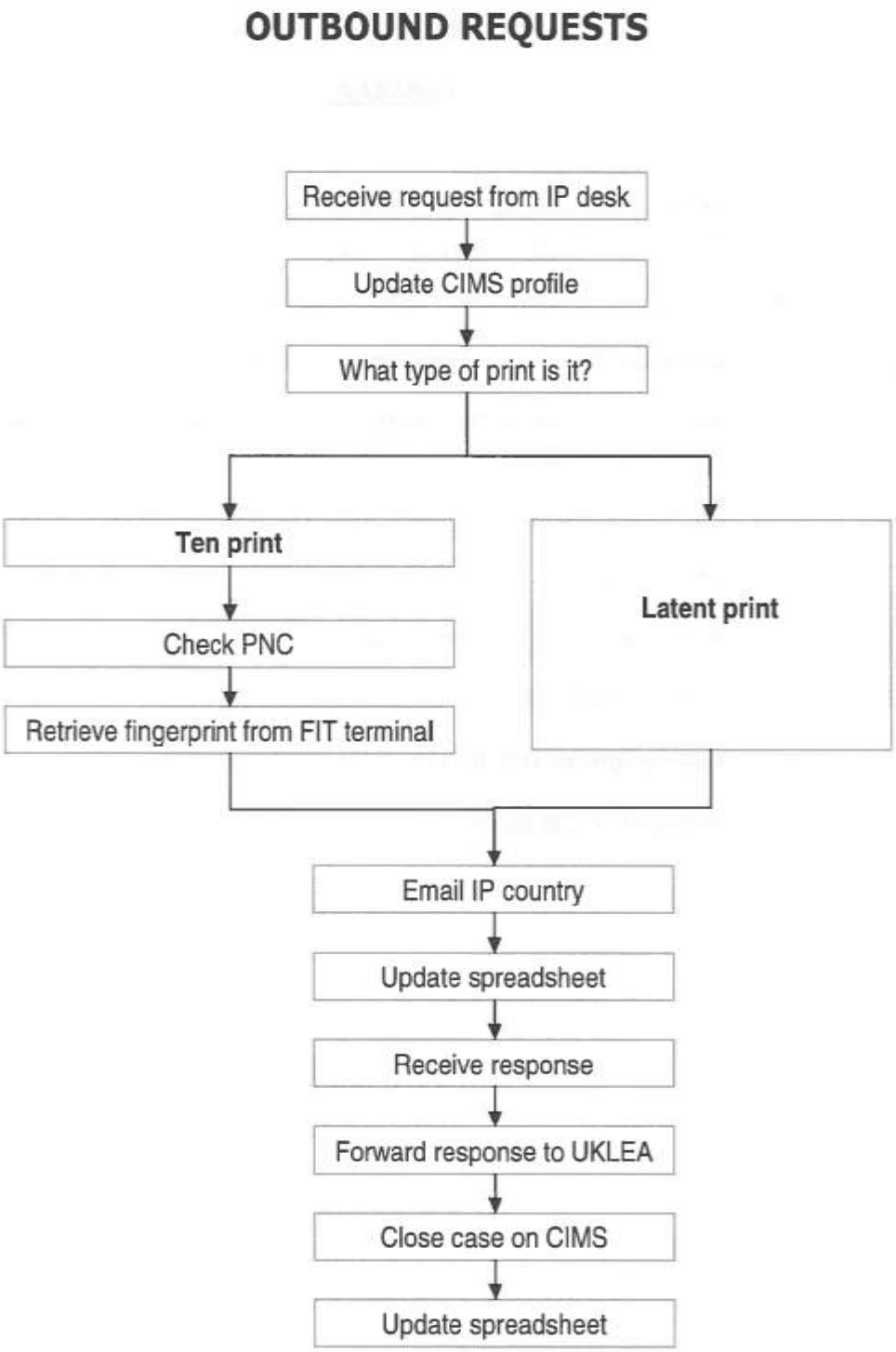
[1] Council Decision 2014/836/EU of 27 November 2014 determining certain consequential and transitional arrangements concerning the cessation of the participation of the United Kingdom of Great Britain and Northern Ireland in certain acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon (see page 11 of this Official Journal).

[2] Council Decision 2007/125/JHA of 12 February 2007 establishing for the period 2007 to 2013, as part of General Programme on Security and Safeguarding Liberties, the Specific Programme 'Prevention of and Fight against Crime' (OJ L 58, 24.2.2007, p. 7).

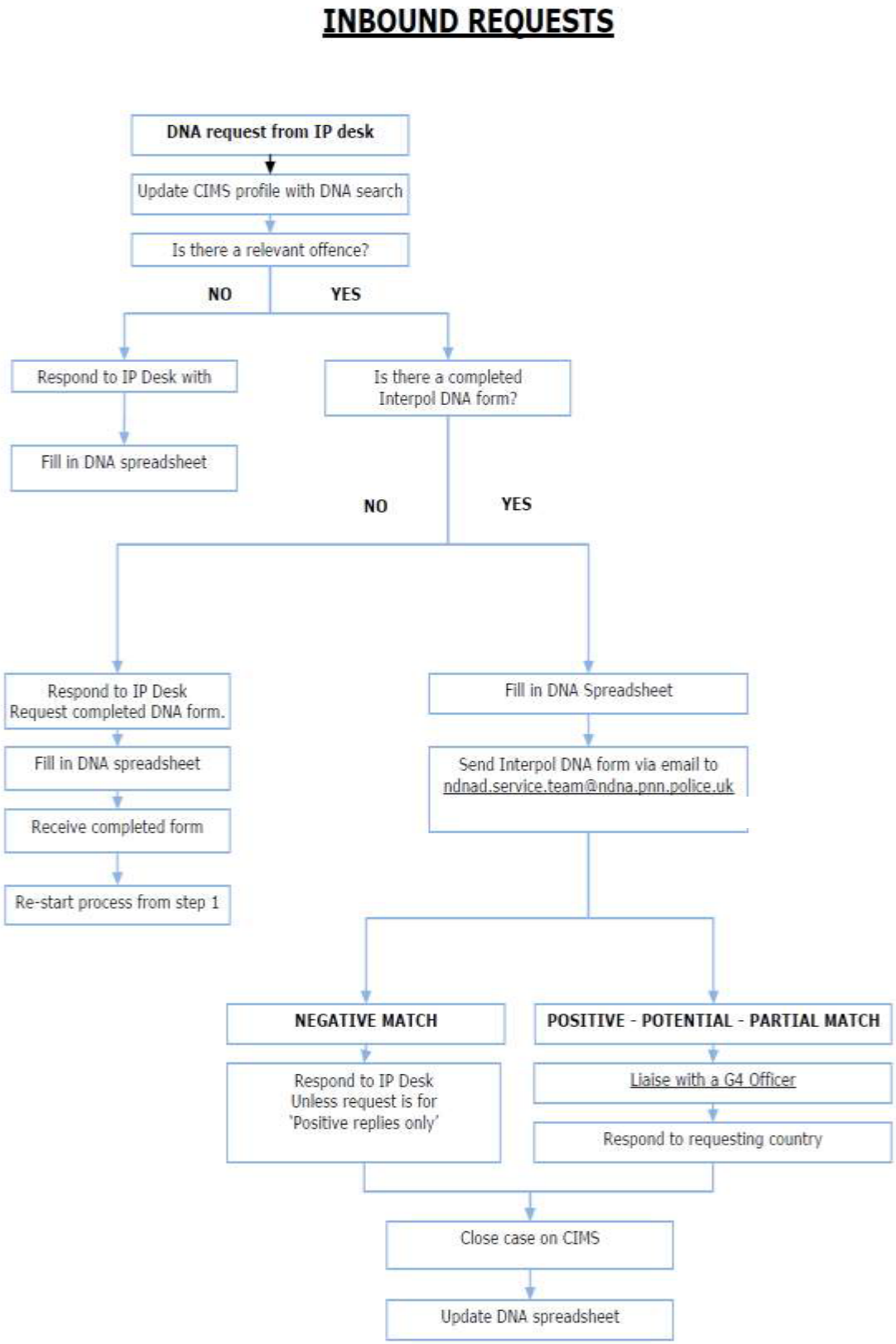
Interpol/NCA current process for Inbound Fingerprints



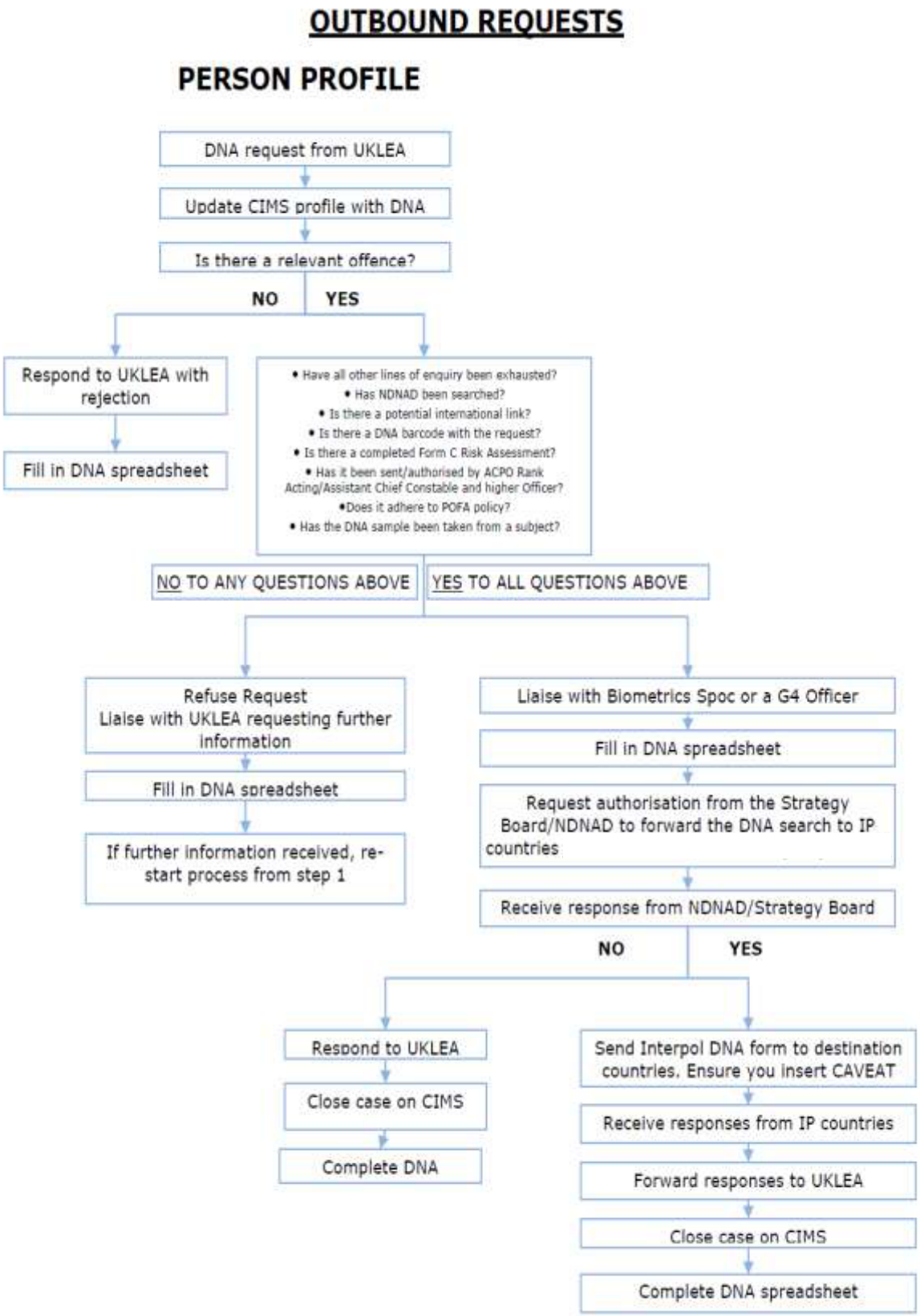
Interpol/NCA current process for Outbound Fingerprints



Interpol/NCA current process for Inbound DNA



Interpol/NCA current process for Outbound DNA



INTERPOL DNA PROFILE SEARCH REQUEST (Version 2)

REQUEST

FROM NCB: Manchester	NCB REFERENCE:
TO NCB:	COPY NCB:
AGENCY REFERENCE:	REQUEST DATE:
NATIONAL AGENCY REQUESTING SEARCH:	

OFFENCE

TYPE OF OFFENCE:	
PLACE OF OFFENCE:	DATE OF OFFENCE:
ADDITIONAL INFORMATION:	

DNA PROFILE INFORMATION

BARCODE (OR NATIONAL DNA PROFILE REFERENCE) :

☐ SUSPECT	☐ CONVICTED	☒ CRIME STAIN
☐ MISSING PERSON	☐ UNIDENTIFIED HUMAN REMAINS	☐ OTHER (PLEASE SPECIFY) :

VWA	THO1	D21S11	FGA	D8S1179	D3S1358	D18S51	Amelogenin
TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539	D2S1338	D19S433
Penta D	Penta E	D1S1656	D2S441	D10S1248	D22S1045	D12S391	SE33
OTHER LOCI							

THIS PROFILE HAS BEEN PRODUCED IN AN ACCREDITED LABORATORY:	☐ YES	☐ NO	☐ UNKNOWN
☐ ISO/IEC 17025	☐ OTHER (PLEASE SPECIFY) :		

IN CASE OF NEGATIVE RESULT STORE AND SEARCH DNA PROFILE:

IN COUNTRIES	☐ YES UNTIL :	☐ NO
IN INTERPOL DNA DATABASE	☐ YES UNTIL :	☐ NO

REPLY

FROM NCB:	TO NCB:	COPY NCB:
NCB REFERENCE:	REPLY DATE:	

THE FOLLOWING RESULT HAS BEEN OBTAINED AFTER THE SEARCH: ☐ POTENTIAL MATCH ☐ NO MATCH

MATCH REPORT NUMBER:	BARCODE (OR NATIONAL DNA PROFILE REFERENCE):

☐ SUSPECT	☐ CONVICTED	☐ CRIME STAIN
☐ MISSING PERSON	☐ UNIDENTIFIED HUMAN REMAINS	☐ OTHER (PLEASE SPECIFY) :

VWA	THO1	D21S11	FGA	D8S1179	D3S1358	D18S51	Amelogenin
TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539	D2S1338	D19S433
Penta D	Penta E	D1S1656	D2S441	D10S1248	D22S1045	D12S391	SE33
OTHER LOCI							

DNA PROFILE RETENTION:

PROFILE STORED AND SEARCHED	☐ YES UNTIL :	☐ NO

INTERPOL UK NCB
Tel: 0207 238 8115
Fax: 0207 238 8112

INTERPOL Enquiry Form

For Help press F1

Protective Marking *:	RESTRICTED		
YOUR DETAILS			
Name + Rank / Grade*:			
Force / Agency*:			
Email*:		Tel No.:	
ILO:		Your Ref*:	
ENQUIRY DETAILS			
Enquiry Type*:	Select	Interpol Ref:	
Category of Enquiry*:	Select	Crime Type*:	
Priority / Urgency*:	Select		
Reason for Priority*:			
Operation Name:			
Destination Countries*:			
Form C Completed:	Select	Authorised By:	
SUBJECT'S DETAILS			
Person:			
Family Name(s):		First Name(s):	
Date of Birth:		Gender:	Select
Nationality:		Place of Birth:	
Name at Birth:		Alias:	
PNC ID:		CRO/CHS No.:	
Additional Information:			
Extra Persons – Please Complete Additional Person Form		Forms attached:	Select
Vehicle:			
Make:		Model:	
VRM:		VIN:	
Country of Registration:		Main Colour:	
Additional Information:			
Extra Vehicles – Please Complete Additional Vehicle Form		Forms attached:	Select
Telephone Number(s):			
No. 1:	No. 2:	No. 3:	No. 4:
Other Subjects: (including Companies, Industrial Equipment, Firearms etc.)			
REQUEST			
CRIMINALITY & ROLE OF THE ABOVE SUBJECTS. Please grade as per the National 5x5x5 Intelligence system. The request will be rejected otherwise.			
REPORT			
Please send via your ILO **If URGENT and ILO is not available - EMAIL TO - manchester@nca.x.gsi.gov.uk**			

Principal Forensic Services Ltd.

Statistical Study: Report

September 2014 v1.3

Dr Gillian Tully & Dr Susan Pope

Contents

With the financial support of the Prevention of and Fight against Crime Programme
European Commission – Directorate-General Home Affairs

Summary of Findings

1. **Recommendations** on composition of profiles that should be exchanged between UK and other EU MS; the basis for the recommendations is discussed in detail in the body of the report.
    a. It is recommended that crime profiles with 8 or more loci (and which have not previously matched against a subject record) be compared against the databases of all other MS, to identify all 8+ locus matches.
    b. Where matches of interest are obtained with 8 or 9 loci, it is recommended that, if sufficient sample remains, the analysis is repeated to increase the number of loci prior to any court proceedings. Although the level of adventitious matches is very low at 8 or 9 loci, upgrading matches to at least 10 loci (the number of loci that have historically been analysed in the UK from 1999 until 2014) is good practice.
        i. It is not possible, ahead of comparison, to identify which UK crime scene profiles will result in 8-locus matches or more: it is inevitable that some 8-locus crime scene profiles from the UK will give matches with fewer than 8 corresponding loci with profiles from other MS. Such matches should be treated in the same way as 6- or 7-locus matches.
    c. There is a chance that any match identified through a database search is adventitious for UK crime scene profiles with 6 or 7 loci, and for international matches with only 6 or 7 loci in common. The number of adventitious matches will depend on the size of the database searched. If the profiles matched share 8 loci fewer adventitious matches would be expected. There are therefore two approaches that could be taken:
        i. For the UK not to share any crime scene profiles with fewer than 8 loci
        ii. For the UK to share all crime scene profiles, and follow up potential matches only where these:
            1. have 8 or more matching loci (and of course no non-matching loci); or
            2. relate to the most serious crimes.

    If the first option is chosen, not to share any crime scene profiles with fewer than 8 loci, the risk is that real matches of interest to UK Policing will not be identified. In France and the Netherlands it has been found that [1,2]:
        - 26-38% of 6-locus matches were true matches;
        - 82-94% of 7-locus matches were true matches.

    We can assume that approximately this range of true 6- and 7-locus matches would be seen in comparisons with UK profiles also.

If the second option is chosen, the risk is one of perception: that the UK had in its possession the information necessary to identify an overseas offender, but did not follow up the lead. However, with this option, there is the potential to follow up leads in serious cases, should resources and priorities permit.

d. Where any 6- or 7-locus matches are obtained and are of interest, it is recommended that reanalysis to increase the number of matching loci is *always* undertaken.
e. In the long term, it would be beneficial if database operators were furnished with software assistance in making decisions with regard to following up retrieved matches. It would be possible to design and implement software to provide the operator with a robust assessment of evidential weight in the form of a likelihood ratio. This measure of value could be combined with a prior probability, based on criminological factors – in particular the existing scale of cross-border crime. Coupled with a measure of utility based on the seriousness of the offence and policy considerations, this would provide an objective aid to decision making. Such software, once validated, would be useful to all MS participating in Prum exchange.
f. It is recommended that the UK shares its subject profiles, but routinely requires at least 10 matching loci prior to releasing demographic details to another country. We understand that only profiles from convicted offenders would be shared; this represents a very high percentage of the total number of subject profiles on the database. The analysis in this report is based on all subject profiles in the database; the level of adventitious matches expected for convicted offenders only would therefore be within a few percent of the totals presented herein. The subject profiles will be full results for the particular multiplex used in their analysis. So, with very few exceptions, these will have 6 (SGM), 10 (SGMPlus) or 16 (DNA17) fully designated loci. SGM profiles have insufficient loci to be included in a search. SGMPlus and DNA17 profiles are suitable for routine searching.
    i. Any SGM profiles for subjects must be upgraded if a Prum search is required
    ii. For exceptional cases, where a very serious crime is involved, consideration could be given to sharing demographic details where there are at least 8 matching loci.

2. **Expected number of true matches** that would be produced when the UK initially engage in Prüm DNA and search their crime scene stains (as a bulk exchange) to other Member States as is required by Prüm.

a. The anticipated match rate in the bulk exchange is in the order of 14,000 true matches, with approximately 3000-4000 true matches annually thereafter.
b. Because France and Germany have the largest databases, these are the countries with which the majority of matches would be expected. However, patterns of cross-border crime may result in a different outcome.
c. The bulk searches do not have to be conducted simultaneously: the search against the database for each MS can be staged. The data provided in this report can be used to inform the order of searches, starting with a smaller MS database to test the protocol, gradually adding those with larger databases that would produce more matches, requiring more resources to follow up.

3. **Expected scale of adventitious matches** if the UK were to engage in Prüm (DNA) with each other MS.
    a. Figures 1 – 4 and Tables 3, 4, 5 and 7 illustrate the expected scale of adventitious matches during bulk exchange and subsequently.
    b. Fewer adventitious matches will be expected for those with 8 loci than for those with 6 or 7 loci.

4. **Any recommended changes to match validation arrangements**
    a. It is recommended that all possible steps are taken to eliminate the potential that a match is due to contamination before it is reported. This will include checking all UK crime scene profiles against an effective elimination database prior to comparison with other MS, and as far as possible, checking any matching crime scene profiles from other MS against available elimination databases prior to reporting matches. Where any gaps exist in elimination databases, reports should be caveated to ensure that the possibility of contamination is considered.
    b. It is therefore recommended that all matching profiles be searched against the UK elimination databases for manufacturers and unsourced profiles before any further action is taken on the match.

Introduction

The Peer Review Group defined the scope of and output from the project on 25/04/2014, as follows:

Scope

1. Developing a model to determine:
    a. The likely impact of the composition of profiles being exchanged from UK to the other European Union (EU) countries, including the consideration of the exchange of incomplete crime scene profiles, the number of loci required for a valid match and the compatibility of the different data sets within the different EU member states (MS).
    b. The likely DNA match rate(s) between the UK and other EU MS, depending on the composition of profiles being exchanged from UK to other EU member states.
2. Developing a model to evaluate the likely scale of adventitious matches if the UK were to engage in Prüm (DNA) with each EU Member State.
3. The work must also consider the partiality of profiles exchanged and the relative likelihood values of DNA matches with other EU MS (subject – subject, stain - stain, stain – subject and subject – stain) and in particular their value to UK law enforcement.
4. Advise the Home Office on other aspects of the Project as required.
5. Review UK procedures for validating matches

Outputs

5. Design of study (delivered)
6. Final Report September 2014 (the present document):
    a. *Summary of findings*: single page list, including:
        i. **Recommendations** to what composition of profiles should be exchanged between UK and other EU MS
        ii. **Anticipated match rate** (e.g. the estimated scale of hits) that would be produced when the UK initially engage in Prüm DNA and search their crime scene stains (as a bulk exchange) to other Member States as is required by Prüm.
        iii. **Expected scale of adventitious matches** if the UK were to engage in Prüm (DNA) with each other MS.
        iv. **Any recommended changes to match validation arrangements**
    b. *Main body*: Basis for recommendations, anticipated match rate and expected scale of adventitious matches
    c. *Appendices*: Supporting information & data

With the financial support of the Prevention of and Fight against Crime Programme
European Commission – Directorate-General Home Affairs

Methods & Data

Data Collection

Questionnaires were designed and sent to Prüm contact points for each of the member states (MS) listed in Table 1. Responses were collated and are provided in full in Appendix 1.

Country	Abbreviation	Response Received
Austria	AT	Full
Cyprus	CY	Partial
Czech Republic	CZ	Full
Estonia	EE	Full
Finland	FI	Full
France	FR	Full
Germany	DE	Full
Hungary	HU	Full
Latvia	LV	None
Lithuania	LT	Full
Netherlands	NL	Full
Poland	PL	Full
Romania	RO	Full
Slovenia	SL	Partial
Spain	ES	
United Kingdom	UK	Full

Table 1: Countries to which requests for data were sent, and responses

Face to face discussions were held with National Database personnel from key MS to gather further detailed information on experiences to date and on processes in place:

1. Kees van der Beek, Custodian for National DNA Database, NL
2. Adam Shariff, DNA Technical Lead, UK National DNA Database (NDNAD)

Information from a French analysis of Prüm matches was obtained from Mathilde Huet, Ministry of the Interior, France [1].

Data Analysis

All assumptions and simplifications are collated in Appendix 2. The project brief was to estimate the "scale" of matches rather than precise numbers. Although we quote numbers (which are all rounded), these should be read as an approximate level (a "scale"), rather than precise numbers, since not all of the assumptions and simplifications can be tested in detail.

Evaluation of the Expected Scale of Adventitious Matches

The expectation for chance matches when databases are compared can be estimated using the formula:

$$Expected\ adventitious\ matches = nNPm$$

where n = the number of records in database 1
N = the number of records in database 2
Pm = the probability of a random match

The probability of a random match (match probability) for any number of DNA markers (loci) is calculated by multiplying together the match probabilities for the individual loci. This calculation makes an assumption that the loci are inherited independently from each other.

When profiles from crime scenes are analysed, not all loci will necessarily yield a result. This may be because the DNA is degraded, or because there is a mixture of DNA from two or more individuals, and not all loci are visible. When not all loci have yielded a result, a "partial" DNA profile is obtained.

To calculate *Pm* for partial profiles, the following method was used:

1. For each number of loci, a random selection from the loci in the multiplex was chosen (using the statistical programming software "R");
2. This random selection of loci was repeated 100 times;
3. For each, the *Pm* was calculated.
4. The mean Pm for each number of loci was calculated as the mean of the *Pm* values for the 100 replicates.

The requirement for this work was to estimate the likely *scale* of adventitious matches rather than to provide an accurate point estimate. Therefore, any deviation from the assumption of independence between loci and the use of an average *Pm* rather than weighting the average to account for some loci being more likely to be missing from partial profiles than others, are unlikely to have a material impact.

Throughout the report, when we refer to an *x*-locus profile or an *x*-locus match, (where *x* can be between 6 and 16), each locus included is a fully designated locus, with no wild-cards. For example, a profile with 8 fully designated loci and one locus containing a wildcard (e.g. "R" for rare allele) would be counted as an 8-locus profile. If this profile were to match with one containing 7 overlapping and fully designated loci and a further locus in which a wildcard was assigned, the match would be a 7-locus match.

Data from Cyprus and Slovenia were not included in the graphs and tables, since an accurate breakdown of partial profiles was not available. The c.1000 profiles from Cyprus analysed using Profiler Plus chemistry would not be suitable for comparison with UK data, as insufficient overlapping loci are present.

Evaluation of the Expected Scale of Adventitious Matches: Bulk Exchange

When a new MS begins Prüm comparisons, a "bulk exchange" is carried out of its entire Prüm database against the entire Prüm database of each other participating MS with which it is exchanging information.

It is in this bulk exchange that the largest number of adventitious matches will be encountered, as it is at this stage that the largest number of comparisons will be performed.

The UK data were compared against each MS for which data were available, as follows:

1. The number of total UK crime scene profiles for each number of loci in the database was decreased to 38% of the number provided, as only crime scene profiles that have not matched against a subject profiles are eligible for Prüm comparison. Currently, this represents 38% of UK crime scene profiles. We have made the simplifying assumption that profiles are equally likely to fulfil this criterion irrespective of the number of loci present.
2. Following equation 1, the comparisons in Table 2 were carried out, to estimate in each case, the number of adventitious matches.
3. Since results for both crime stain and subjects profiled using the DNA17 multiplex have only been accepted for loading onto the UK NDNAD since late July, it is assumed that the UK NDNAD profiles used for the bulk exchange will comprise SGMPlus results with 6-10 loci.

	UK profiles compared	Profiles compared from each MS compared
1	Crime scene profiles with 6-10 loci	Entire MS database
2	Crime scene profiles with 6-10 loci	All MS crime scene profiles
3	All subject profiles	Entire MS database with 6-10+ loci

Table 2: Classes of estimate calculated

Evaluation of the Expected Scale of Adventitious Matches: ongoing exchange

After the bulk exchange has been carried out, the ongoing exchange of data will consist of:

1. Comparison of UK crime scene profiles not already matched against a subject profile against MS databases (Subjects and crime scene profiles). This will include two classes of UK crime scene profiles:
    a. Historic, including those not matched during the bulk exchange or since
    b. Recently added.
2. Comparison of *all* UK subject profiles against recently added MS profiles

We know the composition of the historic profiles, in terms of full and partial profiles, and have used this in the analysis (point 1a above). We cannot know accurately, however, what composition of partial profiles will be obtained in the future (for the analysis in point 1b). We have therefore made an assumption that a similar spread will be achieved as has been achieved historically.

For example, historically, c.78% of crime scene profiles in the UK database are full profiles: we have assumed that this will continue. However, because of the recent adoption of new multiplexes containing 16 rather than the previous 10 loci, a full profile for ongoing exchange will have 16 loci. Similarly, historically, c.6% of crime scene profiles have given 8/10 loci; for ongoing data exchange, under our assumption, this would equate to 6% of recent profiles being 13-locus partial profiles. This is likely to be a worst case scenario, since the new chemistries with 16 loci are substantially more sensitive than the old, 10-locus chemistry.

Evaluation of the expected scale of true matches

It is not possible to statistically evaluate the expected level of true matches, since this depends on criminological factors and not statistical factors. However, in order to provide an estimate of the likely order of magnitude of true matches, observations in countries which have actively been exchanging data over an extended period were studied.

Our analysis and previous work in the Netherlands [2] and France [1] are in close agreement that more adventitious matches occur with 6- and 7-locus matches. With 8 loci and above, c.98% or more of the matches observed will be true matches [1].

To estimate the number of true 6- and 7-locus matches, the ratio of true: false matches from the Netherlands [2] and France [1] were used to extrapolate an estimate of true matches from the expected levels of false matches calculated in this study.

For 8-locus matches and above, the numbers of expected adventitious matches were too small for any such extrapolation. Therefore, the matches observed in the Netherlands were used to extrapolate expectations for the UK:

1. International true matches as a proportion of the total number of international comparisons carried out; and
2. International true matches as a proportion of the number of reported National matches

However, it should be noted that an assumption of a similar pattern of cross-border crime would be required for this extrapolations to be valid. Criminology and patterns of cross-border crime fall outside the remit of this work, and the assumptions have not therefore been validated.

The bulk searches do not have to be conducted simultaneously: the search against the database for each MS can be staged. The data provided in this report can be used to inform the order of searches, starting with a smaller MS database to test the protocol, gradually adding those with larger databases that would produce more matches, requiring more resources to follow up.

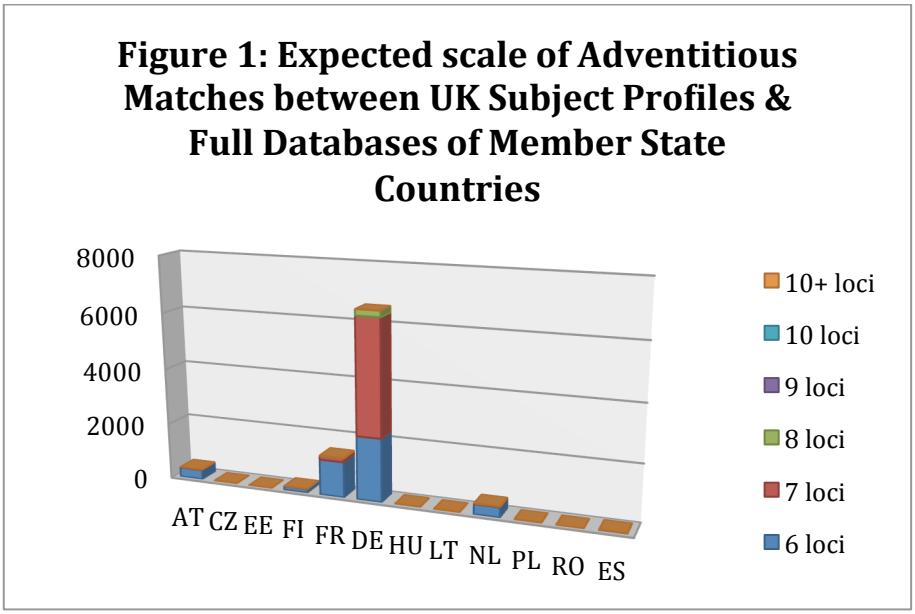
Results

Evaluation of the Expected Scale of Adventitious Matches: Bulk Exchange

Tables 3, 4 & 5 shows the expected scale of adventitious matches as a result of bulk exchange between the UK and other MS in the categories listed in Table 2; these are shown graphically in Figures 1,2 & 3.
Results from Cyprus and Slovenia are not included in the tables, as a detailed breakdown of partial profiles was not available; any instances where expected results from Cyprus or Slovenia are non-zero are noted in the table legends.

Number of Loci	AT	CZ	EE	FI	FR	DE	HU	LT	NL	PL	RO	ES
6	340	10	0	130	1260	2240	20	10	360	10	0	23
7	20	0	0	10	130	4110	0	0	20	0	0	3
8	0	0	0	0	10	220	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0
10+	0	0	0	0	10	0	0	0	0	0	0	1

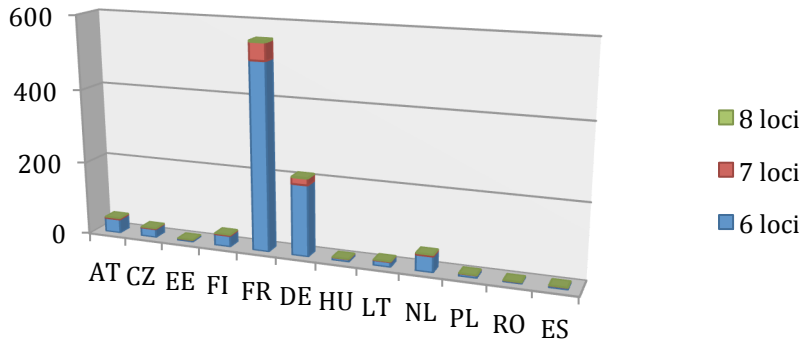
Table 3: Comparison of all UK subject profiles against each MS database in a bulk exchange; rounded to nearest 10. *If all of the Cypriot Powerplex 16 profiles were compared with the UK subject profile database, c.10 adventitious matches may be expected.*



Number of loci	AT	CZ	EE	FI	FR	DE	HU	LT	NL	PL	RO	ES
6	38	23	5	30	504	192	7	14	43	7	4	6
7	4	2	0	3	47	18	1	1	4	1	0	0
8	0	0	0	0	3	1	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0
10+	0	0	0	0	0	0	0	0	0	0	0	0

Table 4: Comparison of all UK crime scene profiles against each MS database in a bulk exchange; rounded to nearest integer

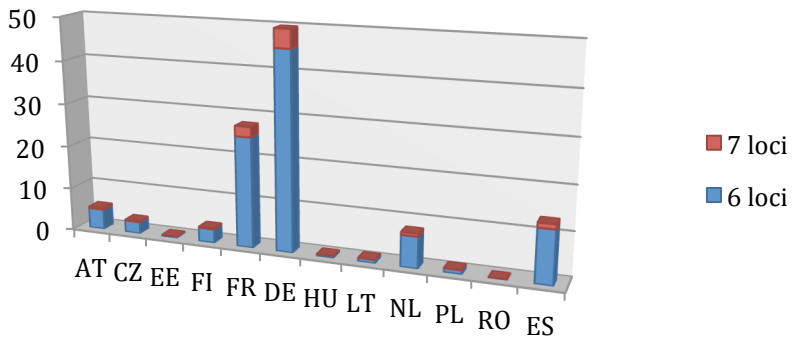
Figure 2: Expected scale of Adventitious Matches between UK Crime Scene Profiles & Full Databases of Member State Countries



Number of loci	AT	CZ	EE	FI	FR	DE	HU	LT	NL	PL	RO	ES
6	5	3	0	3	25	45	0	1	7	1	0	12
7	0	0	0	0	2	4	0	0	1	0	0	1
8+	0	0	0	0	0	0	0	0	0	0	0	0

Table 5: Comparison of all UK crime scene profiles against each MS crime scene profiles in a bulk exchange; rounded to nearest integer

Figure 3: Expected scale of Adventitious Matches between UK Crime Scene Profiles & Crime Scene Profiles of Member State Countries



In order to calibrate the expectations and check for any deviations caused by our assumptions and simplifications, the method used to compare UK data against other MS data was applied to data from the Netherlands, France and Germany. Previous analyses [1] have evaluated the actual number of adventitious matches between these countries, thus enabling our expectations to be compared against reality. The results are shown in Table 6.

Countries Compared	Actual number of adventitious matches	Expected scale of adventitious matches using the methods in this report
FR crime stains vs DE database	211	259
FR crime stains vs NL database	51	57

Table 6: Expected versus observed adventitious matches

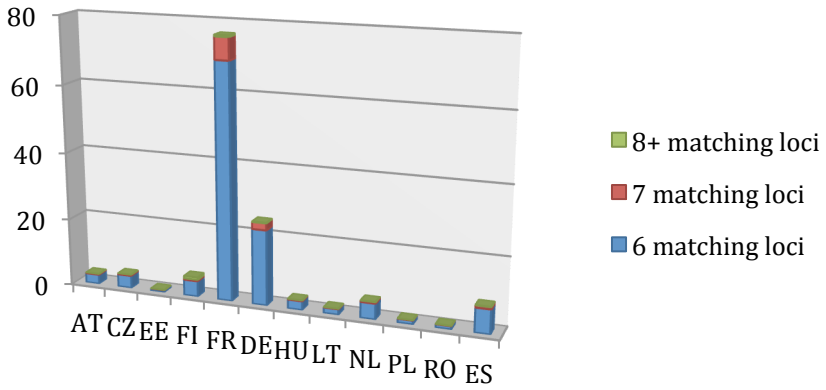
Evaluation of the Expected Scale of Adventitious Matches: ongoing exchange

Table 7 shows the expected annual scale of adventitious matches as a result of ongoing exchange between UK crime scene profiles and other MS; the data are shown graphically in Figure 4.

Number of loci	AT	CZ	EE	FI	FR	DE	HU	LT	NL	PL	RO	ES
6	3	4	1	5	69	22	3	2	5	1	1	7
7	0	0	0	0	6	2	0	0	0	0	0	1
8	0	0	0	1	0	0	0	0	0	0	0	0
9+	0	0	0	0	0	0	0	0	0	0	0	0

Table 7: Comparison of all UK subject profiles against each MS database on an annual basis; rounded to nearest integer

Figure 4: Expected Annual Scale of Adventitious Matches to UK Crime Scene Profiles after Bulk Exchange



Evaluation of the expected scale of true matches

Estimates of the likely scale of true 6- and 7- locus matches, by extrapolation from French and Netherlands proportions of true: adventitious match proportions are shown in Figures 5 & 6 for bulk exchange, and in Figures 7 & 8 on an ongoing annual basis.

Figure 5: Estimate of the Scale of True 6-locus Matches to UK Crime Scene Profiles Expected during Bulk Exchange

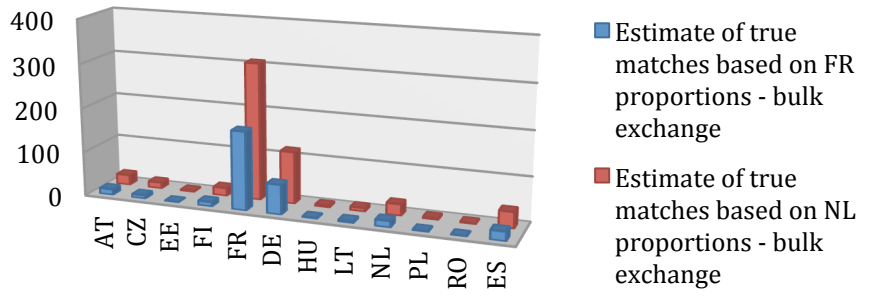


Figure 6: Estimate of the Scale of True 7-locus Matches to UK Crime Scene Profiles Expected during Bulk Exchange

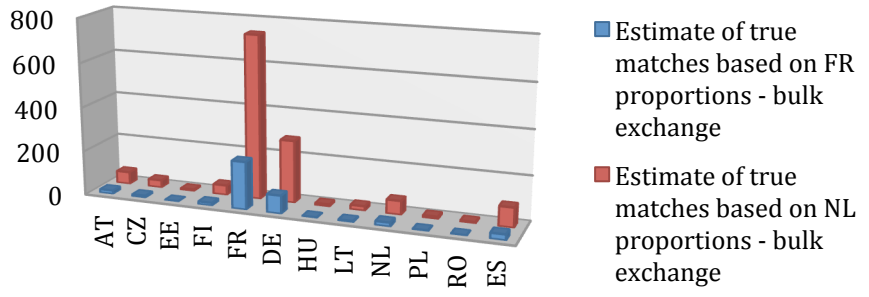


Figure 7: Estimate of the Scale of True 6-locus Matches to UK Crime Scene Profiles Expected Annually after Bulk Exchange

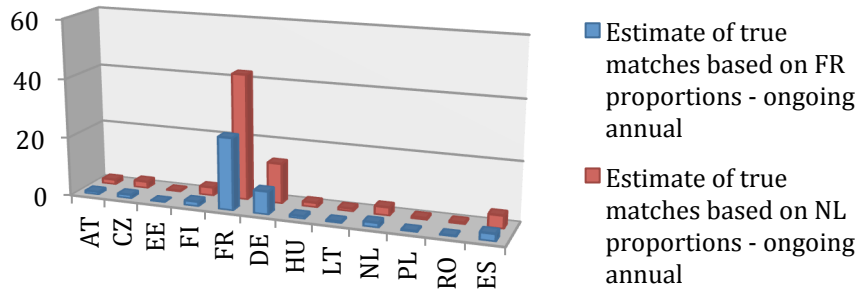
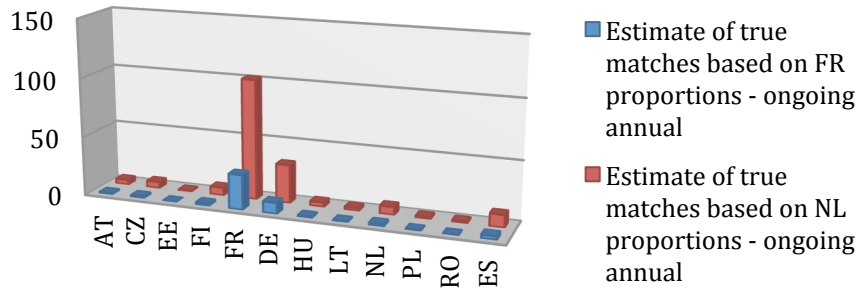


Figure 8: Estimate of the Scale of True 7-locus Matches to UK Crime Scene Profiles Expected Annually after Bulk Exchange



Using the data from the Netherlands on the proportion of comparisons yielding true matches, estimates of the scale of matches:

1. on bulk exchange; and
2. on an ongoing annual basis

by country are given in Figures 9 and 10 respectively.

Figure 9: Estimate of scale of true matches to UK crime scene samples in bulk exchange

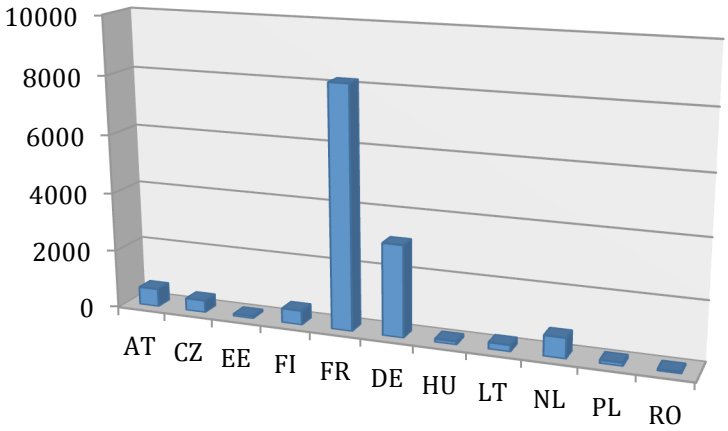
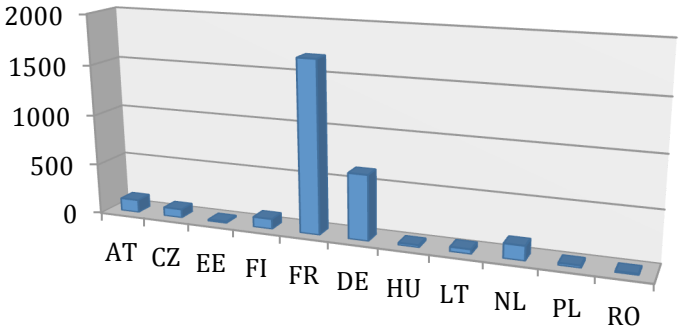


Figure 10: Estimate of scale of true matches to UK crime scene samples annually, after bulk exchange



A second estimate of the likely scale of true matches was provided by Kees van der Beek: in the Netherlands, for every 100 national matches seen, the international matches add a further 20.

For the UK, using data from the NDNAD Annual Report 2012/13, this would equate to approximately 4000 international true matches per year. This estimate is of the same order of magnitude as that shown in figure 10 (total from Fig 10 is approximately 3000).

Discussion & Conclusions

The specification for the current work was to provide **recommendations** on what composition of profiles should be exchanged between UK and other EU MS, an **anticipated match rate** and **expected scale of adventitious matches** if the UK were to engage in Prüm (DNA) with each other MS and **any recommended changes to match validation arrangements.**

Basis of Recommendations on what composition of profiles should be exchanged between UK and other EU MS, and Expected Scale of Adventitious Matches

The work is based on data provided by other MS, and includes a number of assumptions and simplifications as detailed in Appendix 2. We have therefore, where possible, calibrated our results against those observed by MS which have been participating in Prüm data exchange for a number of years. The results presented in Table 3 show the outcome of this calibration, and give confidence that our estimates for the scale of adventitious matches are robust. Nonetheless, they should be seen as an approximation of the level ("scale") of matches and not as precise numerical estimates.

Figure 1 & 2 demonstrate that the number of adventitious matches seen with 8 loci is much lower than for 6 and 7 loci, even where the number of comparisons performed is very large. It is clear, therefore, that the approach to 6- and 7-locus matches should be considered separately from the approach to 8-locus matches and above.

However, it is not possible, ahead of comparison, to identify which UK crime scene profiles will result in 8-locus matches or more: it is inevitable that some 8-locus crime scene profiles from the UK will give matches with fewer than 8 corresponding loci with profiles from other MS. Such matches should be treated in the same way as 6- or 7-locus matches.

Separate consideration will be given to UK crime scene profiles and UK subject profiles: it is likely that the matches to UK crime scene profiles will be of greater significance to UK law enforcement than matches to UK subject profiles; the latter will be of greater value to law enforcement agencies in other MS.

8-locus matches and above: UK crime scene profiles vs. MS databases

The number of adventitious 8-locus matches between UK crime scene profiles and the databases of other MS is expected to be very low (Table 3 and Figure 2). It is therefore recommended that crime profiles with 8 or more complete loci be compared against the databases of all other MS, to identify all 8+ locus matches.

Where matches of interest are obtained with 8 or 9 loci, it is recommended that, if sufficient sample remains, the analysis is repeated to increase the number of loci prior to any court proceedings. Although the level of adventitious matches is very low at 8 or 9 loci, upgrading matches to at least 10 loci (the number of loci that have historically been analysed in the UK from 1999 until 2014) is good practice.

6- and 7-locus matches: UK crime scene profiles vs. MS databases

There is a chance that any match identified through a database search is adventitious for UK crime scene profiles with 6 or 7 loci, and for international matches with only 6 or 7 loci in common. The number of adventitious matches will depend on the size of the database searched. If the profiles matched share 8 loci, fewer adventitious matches would be expected. There are therefore two approaches that could be taken:

1. For the UK not to share any crime scene profiles with fewer than 8 loci
2. For the UK to share all crime scene profiles, and follow up potential matches only where these:
    a. have 8 or more matching loci (and of course no non-matching loci); or
    b. relate to the most serious crimes.

If the first option is chosen, not to share any crime scene profiles with fewer than 8 loci, the risk is that real matches of interest to UK Policing will not be identified. In France and the Netherlands it has been found that [1,2]:

- 26-38% of 6-locus matches were true matches;
- 82-94% of 7-locus matches were true matches.

We can assume that approximately this range of true 6- and 7-locus matches would be seen in comparisons with UK profiles also.

If the second option is chosen, the risk is one of perception: that the UK had in its possession the information necessary to identify an overseas offender, but did not follow up the lead. However, with this option, there is the potential to follow up leads in serious cases, should resources and priorities permit.

Where any 6- or 7-locus matches are obtained and are of interest, it is recommended that reanalysis to increase the number of matching loci is *always* undertaken.

In the long term, it would be beneficial if database operators were furnished with software assistance in making decisions with regard to following up retrieved matches. It would be possible to design and implement software to provide the

operator with a robust assessment of evidential weight in the form of a likelihood ratio. This measure of value could be combined with a prior probability, based on criminological factors – in particular the existing scale of cross-border crime. Coupled with a measure of utility based on the seriousness of the offence and policy considerations, this would provide an objective aid to decision making. Such software, once validated, would be useful to all MS participating in Prum exchange.

UK Subject Profiles: Comparison versus other MS databases

Because the number of comparisons is greater than for crime scene profiles (there are more subject profiles to compare), the expected scale of adventitious matches to UK subject profiles is greater (Figure 1 & Table 3), with a small number of adventitious matches expected even with 10 loci.

Any matches obtained to UK subject profiles are likely to be of primary interest to the MS from which the relevant crime scene stain originated. It would be for this MS to conduct any follow-up analysis, and for the UK to set the standard for the number of loci required in a match before any demographic data from the UK subject would be released.

The bulk searches do not have to be conducted simultaneously: the search against the database for each MS can be staged. The data provided in this report can be used to inform the order of searches, starting with a smaller MS database to test the protocol, gradually adding those with larger databases that would produce more matches, requiring more resources to follow up.

It is recommended that the UK shares its subject profiles, but routinely requires at least 10 matching loci prior to releasing demographic details to another country. We understand that only profiles from convicted offenders would be shared; this represents a very high percentage of the total number of subject profiles on the database. The analysis in this report is based on all subject profiles in the database; the level of adventitious matches for convicted offenders only would therefore be expected to be approximately the same as the totals presented herein. The subject profiles will be full results for the particular multiplex used in their analysis. So, with very few exceptions, these will have 6 (SGM), 10 (SGMPlus) or 16 (DNA17) fully designated loci. SGM profiles have insufficient loci to be included in a search. SGMPlus and DNA17 profiles are suitable for routine searching.

i. Any SGM profiles for subjects must be upgraded if a Prum search is required

ii. For exceptional cases, where a very serious crime is involved, consideration could be given to sharing demographic details where there are at least 8 matching loci.

Basis of anticipated match rate that would be produced when the UK initially engage in Prüm DNA and search their crime scene stains (as a bulk exchange) to other Member States

Using data from other MS to estimate the scale of true matches to be expected relies on an assumption that cross-border patterns of crime are the same between the Netherlands (for which we have the greatest granularity of data), France (for 6- and 7-locus matches) and the UK are similar. We cannot substantiate this assumption, and so the estimates of true matches provided should be treated with caution.

The two different methods of estimating an approximate scale of true matches from Netherlands data (one based on a proportion of the total number of international comparisons and the other on a proportion of national matches) gave results that were of the same order of magnitude (c. 3000 vs c.4000 per annum after bulk exchange), which provides assurance that the methods used were valid. This provides, however, no information regarding the cross-border patterns of crime.

Match Validation Arrangements

The most important recommendation in relation to match validation arrangements is that the possibility of DNA contamination of a result, usually a crime stain, should always be considered, and as far as possible eliminated, prior to reporting a match and ideally before the profile is even included in the data exchange.

In the UK, plans are in progress to create and maintain a high quality suite of elimination databases, covering forensic service provider staff, police staff, medical examiners, staff from manufacturers of consumables and unsourced contaminants. As of September 2014, the Forensic Science Regulator has an agreed protocol for England and Wales in place, which will be implemented from April 2015 [3]. Although individual countries and FSPs hold elimination databases for their own scientific staff as well as manufacturers, there is not at this point a pan-European equivalent database. The DNA Working Group of the European Network of Forensic Science Institutes (ENFSI) is continuing to work towards shared manufacturers and unsourced contaminants databases.
An unsourced contaminants database is held by the International Commission on Missing Persons (ICMP, Sarajevo) [4]. This includes DNA profiles that are detected in control samples that must be due to extraneous contaminating DNA.

Many are later sourced as being from manufactured consumables and solutions used in the process of recovering samples for DNA analysis.

It is recommended that all possible steps are taken to eliminate the potential that a match is due to contamination before it is reported. This will include checking all UK crime scene profiles against an effective elimination database prior to comparison with other MS, and as far as possible, checking any matching crime scene profiles from other MS against available elimination databases prior to reporting matches. Where any gaps exist in elimination databases, reports should be caveated to ensure that the possibility of contamination is considered.

It is therefore recommended that all matching profiles be searched against the UK elimination databases for manufacturers and unsourced profiles before any further action is taken on the match.

Acknowledgements

This report was prepared with the financial support of the Prevention of and Fight against Crime Programme of the European Commission (Directorate-General Home Affairs).

The authors wish to give particular thanks to Kees van der Beek (NFI), Adam Shariff (NDU), Nick Apps and Gary Linton (SCJS) for useful discussion of database and Prüm exchange issues, and to Mathilde Huet (MoI, France), Roberto Puch-Solis (LGC Forensics) and Ian Evett (PFS) for their insight and assistance in relation to the statistical analysis.

We thank the following individuals for provision of data on which this report is based: Reinhard Schmid (AT), Marios Cariolou (CY), Alice Reslova (CZ), Aivi Sootla (EE), Emilia Lindberg (FI), Alain M. Mesmoudi (FR), Alexander Bachmann (DE), Zoltan Kormos (HU), Jelena Kolesnikova (LT), Kees van der Beek (NL), Jakub Mondzelewski (PL), Florin Stanciu (RO), Katja Drobnic (SI), Caroline Goryll (NDU, UK)

Abbreviations (and definitions)

Adventitious match	DNA profiles from two individuals, who are not identical twins, that match by chance.
Allele	Alternative forms of a DNA sequence at a particular locus

DNA17	DNA multiplex that contains all the loci specified by ENFSI
ENFSI	The DNA Working Group of the European Network of Forensic Science Institutes
FSP	Forensic Science Provider
ICMP	International Commission on Missing Persons
Locus (pl.loci)	Specific location of a DNA sequence on a chromosome; for forensic analysis it refers to areas that vary between individuals
MS	Member State
Multiplex	DNA system that simultaneously analyses several loci in a single test
NDNAD	National DNA Database
NDU	National DNA Database Delivery Unit (UK)
SGMPlus	Second Generation Multiplex Plus (standard UK multiplex from 1999 – 2014)
Wild card	An undesignated placeholder included where the presence of an allele is uncertain but needs to be considered

References

[1] Huet, Mathilde. A study of the false positives in the French DNA database and simulations, presentation at PIES conferences, NICC, Belgium, 25 June 2014

[2] van der Beek , Kees. (Custodian Dutch DNA-database). The implementation of the Prüm Treaty/EU-Council Decisions in the Netherlands, presentation at Metropolitan Police Prum meeting, London on 16 May 2014:

[3] Forensic Science Regulator Codes of Practice and Conduct: Protocol: DNA contamination detection -The management and use of staff elimination DNA databases SR-P-302 ISSUE 1

[4] International Commission on Missing Persons (ICMP) Online Elimination Database Matching Application (*https://edb.ic-mp.org/index.php?w=intro&l=en*)

Appendix 1: Data Returns from Member States

Data Request: Austria

Provided by: Reinhard.Schmid@bmi.gv.at

Data provided as of 24/07/2014		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	25.320 (open stain profiles for Prüm searches)
	b. Suspect profiles	179.772
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	1.361 (stains) 0 (reference)
	7	989 (stains) 2 (reference)
	8	1.197 (stains) 3(reference)
	9	1.578 (stains) 208 (reference)
	10	11.871 (stains) 125.473 (reference)
	11	423 (stains) 0 (reference)
	12	435 (stains) 0 (reference)
	13	516 (stains) 1(reference)
	14	617 (stains) 6 (reference)
	15	798 (stains) 376 (reference)
	16	5.535 (stains) 53.703 (reference)
	>16	0
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		SGM (1997-1998) SGM+ (1999-2010) NGMSE (since 2011)
Standard Practice regarding upgrading potential matches (processing additional loci)		Upgrade of each reference profile in case of a hit (national as well as in Prüm) to actual used quality

With the financial support of the Prevention of and Fight against Crime Programme
European Commission – Directorate-General Home Affairs

	(presently NGMSE). Upgrade of stains if necessary and if biological material is available.
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database	No duplicated profiles since 2004 possible because of one times acquisition policy (controlled with fingerprint checks by 24/7 realtime data transmission and AFIS search procedures in Austrian .BK). After profile upgrade the better quality profile will be searched automated again also in Prüm network but with same profile number (only additional underline version number changes. This number refers to number of quality upgrade).
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)	Only identical twins and multiple siblings will be enumerated and controlled. No statistics about other status of relatives are claimed.
Historical growth rate and projected growth rate of database	Each year about 13.000 new reference profiles and about 2000 new loaded open stains with Prüm quality and without national hits to national reference profiles (Prüm stain profiles)
Any "binning" and wildcards (including, if applicable, rare alleles) used	Of course. Provided in Prüm in accordance with existing quality definition and data structure of Prüm Decision

Data Request: Cyprus

Provided by: cariolou@cing.ac.cy

Data provided as of 31 December 2013		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	10.765
	b. Suspect profiles	335 (only convicted persons)
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	
	7	
	8	
	9	
	10	
	11	~ 1.000
	12	
	13	
	14	
	15	~ 9.765
	16	
	>16	
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		ProfilerPlus (~1.000) PowerPlex-16 (~9.765)
Standard Practice regarding upgrading potential matches (processing additional loci)		Additional loci may be typed on reference profiles or if additional crime scene profiles are available. This is done on serious cases.
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		No duplicates allowed in Cypriot Prum database.
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)		No available estimates but we expect that this should be negligible.
Historical growth rate and projected growth rate of database		Difficult to estimate. For crime scene profiles perhaps 100-300 year. Much less for convicted persons.
Any "binning" and wildcards (including, if applicable, rare alleles) used		No binning nor wildcards included in database.

Data Request: CZECH REPUBLIC

Provided by: alice.reslova@pcr.cz

Data provided as of 21/08/2013		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	14 576
	b. Suspect profiles	2 404 (Suspects) 121 822 (Offenders)
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	31
	7	31
	8	116
	9	250
	10	5 207
	11	485
	12	331
	13	609
	14	1 305
	15	66 536
	16	58 545
	>16	6 060
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		PowerPlex 16, Identifiler (2002-2010) PowerPlex ESI 17, ESX 17, NGM (2010-2014) 50 981 = PowerPlex 16 15 556 = Identifiler 58 513 = ESI 17, ESX 17 2 634 = NGM 11822 = reanalysed profiles (mix of several kits)
Standard Practice regarding upgrading potential matches (processing additional loci)		Additional loci are analysed by all profiles from potential matches (if profiles are still available). If profiles are not available, raw data of profile are checked and the calculation of match probability is

	provided to police authority with the note about necessity of other verification of all relevant case information.
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database	Estimation is about 100 profiles, but duplicated profiles are continuously deleted from the database.
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)	Profiles of close relatives are not the part of Prüm comparison database, but in the rest of the whole database there are currently 420 profiles of close relatives.
Historical growth rate and projected growth rate of database	2002 – 2006 = 17304 profiles included to the database 2007 – 2009 = 47259 profiles included (mass collection of DNA profiles from prisoners) Since 2010 to this day the increment of profiles in the database is cca 20 000 profiles per year. The current number of all profiles in Czech DNA database is 158 892.
Any "binning" and wildcards (including, if applicable, rare alleles) used	We do not use any "binning" or wildcards. All alleles including microvariants are inserted into the database and if some allele is questionable we do not insert it at all.

Data Request: ESTONIA

Provided by: aivi.sootla@ekei.ee

Data provided as of 10/06/2014		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	1712
	b. Suspect profiles	26 088
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	-
	7	-
	8	-
	9	4
	10	21263
	11	-
	12	2
	13	2
	14	-
	15	6357
	16	7
	>16	165
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		Most of the profiles with 10 loci – SGM Plus. Most of the profiles with 15 loci – PowerPlex ESI 16.
Standard Practice regarding upgrading potential matches (processing additional loci)		If external profile has more loci and if possible - always process additional loci.
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		Person profiles – few, if any. Stain profiles – some, exact number not known.
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)		No estimates
Historical growth rate and projected growth rate of database		1618 new profiles in 2014 (until 10.06.2014)
Any "binning" and wildcards (including, if applicable, rare alleles) used		Rare alleles – numerical value in database, if possible.

Data Request: FINLAND

Provided by: Emilia Lindberg, bio.rtl.krp@poliisi.fi

Data provided as of 21/05/2014		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	17 029
	b. Suspect profiles	145 828
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	517
	7	808
	8	990
	9	1 423
	10	129 725
	11	148
	12	209
	13	415
	14	1 100
	15	27 522
	16	-
	>16	-
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		AmpF∫STR SGM Plus: between Dec 1999 and Jun 2012 Investigator ESS Plex Plus: since Jun 2012
Standard Practice regarding upgrading potential matches (processing additional loci)		Person profiles can be upgraded with Investigator ESS Plex loci
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		None
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)		N/A
Historical growth rate and projected growth rate of database		~25 000/year
Any “binning” and wildcards (including, if applicable, rare alleles) used		Over marker range alleles marked with < or >

With the financial support of the Prevention of and Fight against Crime Programme
European Commission – Directorate-General Home Affairs

Data Request: FRANCE

Provided by: alain.mesmoudi@gendarmerie.interieur.gouv.fr

Data provided as of 06/02/2014		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	137,140
	b. Suspect profiles	2,586,727
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	4,997
	7	7,916
	8	8,158
	9	7,744
	10	175,312
	11	7,125
	12	8,281
	13	15,308
	14	75,794
	15	2,082,655
	16	20,572
	>16	17: 309,884 18: 121
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		AmpFℓSTR® Sefiler™ AmpFℓSTR® COfiler™ AmpFℓSTR® Identifiler® Investigator™ Idplex® Investigator™ Idplex Plus® AmpFℓSTR® NGM™ PowerPlex® PowerPlex® 16 PowerPlex® 18D PowerPlex® 21 PowerPlex® ES PowerPlex® ESI 16 PowerPlex® ESI 17 PowerPlex® ESX 16 PowerPlex® ESX 17 AmpFℓSTR® Profiler® AmpFℓSTR® Profiler Plus® AmpFℓSTR® SGM Plus®
Standard Practice regarding upgrading potential matches (processing additional loci)		No upgrading

With the financial support of the Prevention of and Fight against Crime Programme
European Commission – Directorate-General Home Affairs

Estimated number of duplicated profiles (if any) profiles in Prüm comparison database	We know that we have some but we don't know how many
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)	We don't have this information
Historical growth rate and projected growth rate of database	375000 new profiles in 2013
Any "binning" and wildcards (including, if applicable, rare alleles) used	For some profiles we have only one allele known, it is represented as "-". For instance, if for some locus we have one value known, let's say 17, the locus is set as "17, -"

Data Request: GERMANY

Provided by: alexander.bachmann@bka.bund.de

Data provided as of 05/06/2014		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	245,408
	b. Suspect profiles	791,598
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	8,906
	7	250,481
	8	302,189
	9	3,340
	10	10,774
	11	124,962
	12	1,360
	13	13,146
	14	3,666
	15	8,755
	16	308,840
	>16	587
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		There was never a regulation determining the kits in use. The data were generated using practically every kit on the forensic market including self-made. Most of the data are results of two independent amplifications preferably with two different kits. The number of false homozygotes is expected to be low. Analysis kits used are not linked to the profiles.
Standard Practice regarding upgrading potential matches (processing additional loci)		No Standard Practice for upgrading potential matches in Germany.

Estimated number of duplicated profiles (if any) profiles in Prüm comparison database	None. Every profile belongs to a separate criminal case.
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)	There are no estimates how many close relatives are criminal offenders and at the same time in the database.
Historical growth rate and projected growth rate of database	Historical growth rate: 8,000-10,000 profiles a month Actual growth rate: 5,000-8,000 profiles a month Projected growth rate: 4,000-5,000 profiles a month
Any "binning" and wildcards (including, if applicable, rare alleles) used	No "binning". Wildcards are only used for rare alleles (values below the "normal" range = "1" and values above the range = "99").

Data Request: HUNGARY

Provided by: Zoltan Kormos - dna.database@orfk.police.hu

Data provided as of 12 June 2014		
Number of profiles in Prüm comparison database	a. Scene of Crime profiles	2.387
	b. Suspect profiles c. Convicted Offender profiles	21.072 14.275
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	61
	7	92
	8	129
	9	592
	10	565
	11	62
	12	90
	13	124
	14	170
	15	35731
	16	112
	>16	6
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		See Table 1.
Standard Practice regarding upgrading potential matches (processing additional loci)		Every match candidate originating from automated DNA data exchange among Prum partners will be checked by qualified experts of the Hungarian National DNA Database. The validation process is carried out according to the ENFSI DNA database management recommendations, which in many cases contains additional DNA analysis before notification is made.
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		0

With the financial support of the Prevention of and Fight against Crime Programme
European Commission – Directorate-General Home Affairs

Any available estimates of numbers of close relatives on the databases (siblings and parent/child)	No data
Historical growth rate and projected growth rate of database	See Table 2.
Any "binning" and wildcards (including, if applicable, rare alleles) used	We use multiplex kit specific > and < bins for out of ladder range alleles. No wildcards are currently in use.

Table 1.

Multiplex Kit	Number of Personal DNA Profiles	Number of Scene of Crime DNA Profiles *	Period in use
Profiler Plus	0	505	1998 - 2010
COfiler	0	34	1999 -2006
Identifiler	12.533	17	2001 - 2014
MiniFiler	0	32	2007 - 2012
SGM Plus	0	757	2009 - 2012
NGM	9.007	800	2009 - 2014
NGM SElect	0	130	2012 - 2014
PowerPlex 16	0	7	2000 - 2008
PowerPlex ESI 16	13.807	165	2011 - 2014
PowerPlex ESI 17	0	34	2009 - 2014

* As some Scene of Crime DNA profiles managed in Prum database has been produced by the use of multiple kits, the sum of given profiles is more than the actual number of profiles they were generated from (2.387).

Table 2.

Date	30.06. 2012	30.09. 2012	31.12. 2012	31.03. 2013	30.06. 2013	30.09. 2013	31.12. 2013	31.03. 2014	12.06. 2014
Number of Scene of Crime DNA Profiles	115	358	478	482	480	473	1.734	2.142	2.387
Number of Personal DNA Profiles	18.291	14.441	13.864	21.588	23.681	27.096	30.242	32.849	35.347

First Prum search date: 19.09.2012 with AT.

Data Request: LITHUANIA

Provided by: Jelena.Kolesnikova@policija.lt

Data provided as of 14/04/2014		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	4080
	b. Suspect profiles	70541
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	34
	7	144
	8	364
	9	4510
	10	45399
	11	50
	12	116
	13	503
	14	352
	15	22870
	16	36
	>16	243
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		AmplFlSTR SGM Plus (not in use since Dec 2011) 45399 profiles, AmplFlSTR Identifiler 1056 profiles, AmplFlSTR Minifiler 3 profiles, AmplFlSTR NGM 28127 profiles, AmplFlSTR NGM Select Express 36 profiles.
Standard Practice regarding upgrading potential matches (processing additional loci)		If possible, re-amplification with NGM kit (DNA extracts are stored up to 10 years)
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		1433 duplicated profiles of suspect's
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)		N/A
Historical growth rate and projected growth rate of		Approx. 700 stain's

database	profiles and 8000 suspect's profiles per year are included into database.
Any "binning" and wildcards (including, if applicable, rare alleles) used	N/A

Data Request: NETHERLANDS

Provided by: k.v.d.beek@nfi.minvenj.nl

Data provided as of 10/07/2014		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	38,678
	b. Suspect profiles	191,338
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	1,418
	7	934
	8	1,671
	9	4,214
	10	125,972
	11	519
	12	459
	13	1,205
	14	6,778
	15	85,919
	16	223
	>16	1,553
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		NGM since May 2013
Standard Practice regarding upgrading potential matches (processing additional loci)		Each 6 or 7 locus match which is of interest to NL is typed with additional loci
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		450
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)		No data
Historical growth rate and projected growth rate of database		Current total is c. 200000. Expected to include 25000 persons per annum from 2014 onwards, and from 2022, will start to remove profiles, leading to a steady state total number of profiles of c.625000 persons in t0tal by 2034.
Any “binning” and wildcards (including, if applicable, rare alleles) used		None

With the financial support of the Prevention of and Fight against Crime Programme
European Commission – Directorate-General Home Affairs

Data Request: POLAND

Provided by: jakub.mondzelewski@policja.gov.pl

Data provided as of 30/04/2014		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	4791
	b. Suspect profiles	33890
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	23
	7	69
	8	122
	9	240
	10	29584
	11	60
	12	37
	13	69
	14	168
	15	7941
	16	282
	>16	86
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		SGMplus – from 2007 to the end of 2012. NGM or NGMSElect since 2013
Standard Practice regarding upgrading potential matches (processing additional loci)		If possible, profiles are upgrading to 15 or 16 loci. Kit: NGM or NGMSElect
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		0
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)		32
Historical growth rate and projected growth rate of database		c.a. 6000 profiles per year
Any “binning” and wildcards (including, if applicable, rare alleles) used		No

Data Request: ROMANIA

Provided by: Florin Stanciu, criminalistica@politiaromana.ro

Data provided as of 17/07/14			
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	801	
	b. Suspect profiles	suspects: 702 convicted offenders: 20,916	
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	7 crime	7
	7	16	16
	8	72	72
	9	160	160
	10		352
	11		380
	12		543
	13		1008
	14		2278
	15		16150
	16		1479
	>16		12
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		ESSplex - 5974 ESSplex SE - 2413 Nonaplex - 32 Identifiler - 14028	
Standard Practice regarding upgrading potential matches (processing additional loci)		If we have a copy of the original profile, standard procedure implies reprocessing the profile	
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		22	
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)		32	
Historical growth rate and projected growth rate of database		c. 5000 per year	
Any “binning” and wildcards (including, if applicable, rare alleles) used		-	

Data Request: SLOVENIA

Provided by: katja.drobnic@policija.si

Data provided as of 01/12/2013		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	6,356
	b. Suspect profiles	27,534
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	
	7	
	8	
	9	
	10	33,890
	11	
	12	
	13	
	14	
	15	
	16	
	>16	
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		SGMplus until 2011, then NGM
Standard Practice regarding upgrading potential matches (processing additional loci)		
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)		
Historical growth rate and projected growth rate of database		
Any “binning” and wildcards (including, if applicable, rare alleles) used		

Data Request: UK

Provided by: Caroline.Goryll@homeoffice.pnn.police.uk

Data provided as of 01/07/2014		
Number of profiles in Prüm comparison database:	a. Scene of Crime profiles	170,175
	b. Suspect profiles	5,599,335
Number of profiles with 6….n loci, where n = maximum loci (excluding Amelogenin)	6	4,122
	7	5,910
	8	9,869
	9	17,282
	10	132,426
	11	
	12	
	13	
	14	
	15	
	16	
	>16	
Multiplex kit(s) used, with dates in use and associated number of profiles in Prüm comparison database		SGMPlus
Standard Practice regarding upgrading potential matches (processing additional loci)		
Estimated number of duplicated profiles (if any) profiles in Prüm comparison database		
Any available estimates of numbers of close relatives on the databases (siblings and parent/child)		Unable to provide
Historical growth rate and projected growth rate of database		Previous years from annual reports 13/14 figures:- Crime Scene loads - 35005 Subject loads - 361933 Crime scene deletions - 6837 Subject deletions – 1,384,905 Previous years from annual reports 13/14 figures:- Crime Scene loads - 35005

	Subject loads - 361933 Crime scene deletions - 6837 Subject deletions – 1,384,905 Previous years from annual reports 13/14 figures:- Crime Scene loads - 35005 Subject loads - 361933 Crime scene deletions - 6837 Subject deletions – 1,384,905
Any "binning" and wildcards (including, if applicable, rare alleles) used	From 1999 to 14th November 2008 the pre-3.3b rules were in place for Th01 binned alleles such that a Th01 10 would be assigned a value 'R' for loading to the NDNAD – full details of the legacy arrangements are in 2008 version of the Technical Standards document. (Both the legacy document and current document included below. Since this point FSPs have been back-converting 'R' to numerical designations for NDNAD retained records. A further minor change has been introduced since 1st February 2014 where vWA alleles 22, 23, 24 and 25, (and any variants of) though callable by the SGMPlus had until this point needed to be assigned a wildcard 'R' (to account for potential SGM vWA/FGA crossover) – from 1st February 2014 these alleles are to be assigned with the numerical value.

Appendix 2: Assumptions & Simplifications

1. The numbers quoted are all based on the match probabilities for the White Caucasian population since it is assumed that this is the largest population group across Europe
2. The match probabilities are taken from US White Caucasian data for DNA17 systems and it is assumed that these are appropriate for the European White Caucasian population
3. The numbers are based on the average probability of a match
4. The calculations assume independent inheritance of DNA loci
5. We have adjusted the number of UK crime scene profiles to "remove" all those already matched to a subject profile. In doing so, we have assumed that the proportion of partial profiles in the remaining set mirrors that in the crime scene database as a whole
6. For the purpose of estimating matches in future when the UK uses DNA17 systems, it is assumed that the proportion of crime results that are partial profiles will remain constant. That is, it is assumed that the proportion of the 16 DNA17 loci (not including Amelogenin) obtained is the same as that of the 10 SGMPlus loci. So an SGMPlus crime result with 8 loci would be the equivalent of a DNA17 crime result with 13 loci. About 6% of current SGMPlus crime profiles have 8 loci so 6% of future loads of DNA17 crime profiles will have 13 loci
7. Each number of loci quoted refers to fully designated loci and not loci containing wildcards
8. We assume that relatives and duplicates present within databases are at such a low level as to have negligible impact on the analysis.
9. The eligible unmatched crime results from the UK have been compared against the crime and subject profiles of other MS with no breakdown of crime types
10. It is assumed that all partial profiles are from crime stains and not subjects for those MS where this information could not be provided. The actual figures are given for Austria and Germany
11. In estimating the scale of true matches, an assumption that the UK pattern of cross-border crime emulates that of the NL is required

Appendix 3: Supporting information and data

Prüm Inclusion Rules

The criteria that DNA results have to reach to be included in international comparisons are that the profile:
- Must include at least 6 of the 7 old ESS loci for subjects
- Must include at least 6 ESS loci for crime scene stains
- Must include any other of the 24 old1 Interpol loci
- One allele of a locus can be a wildcard
- No mixed profiles (a maximum of two values per locus) are allowed
- No profiles that have already matched a person are allowed
- No profiles that a country does not want to make available are allowed (e.g., DNA profiles of laboratory personnel kept for contamination detection purpose)

Prüm Matching Rules

The software produces a match when there are at least six fully matching loci between two DNA profiles. In addition, one deviation (wildcard or mismatch) is allowed, and this is called a near match. Any type of profile sent for a comparison will be compared to any type of DNA profile available for comparison, so the following types of matches can occur: stain-stain, stain- person or person-person. The matches can be of four different qualities:
Quality 1: All alleles of all loci that can match are identical
Quality 2: One of the two matching profiles contains a wildcard
Quality 3: One of the alleles of one locus contains a mismatch of one base pair (e.g., 9.2 ↔ 9.3)
Quality 4: One of the alleles of one locus contains a mismatch of more than one base pair (e.g., 22 ↔ 26)

Reports on visits

- **NDNAD Delivery Unit (NDU)**

Sue Pope visited Adam Shariff (DNA Technical Lead) and Caroline Goryll (data analyst) at Vienna House, Birmingham on 29 May 2014. They discussed the provision of data by NDU. The request was put to the National DNA Database Strategy Board at their meeting in June and accepted. The meeting also covered the current and planned rules on designation of wild cards, rare alleles and somatic mutations as well as policy on duplicate subject and crime profiles.

- **Netherlands Forensic Institute (NFI)**

Gill Tully and Sue Pope visited Kees van der Beek (Netherlands National DNA Database Manager) at the NFI on 12 June 2014. This included the opportunity to

watch and discuss the daily review, process and actions for the Prum database search hits involving the Netherlands.
We were also provided with data about the types and numbers of hits including a review of 100 Quality 3 & 4 cases that were followed up with further analysis. This real data was used to assess the reliability of the estimates produced using the adventitious match rate model.
Other data provided was the breakdown of matches in different categories, including the proportion of matches to foreign stains that were from NL residents born abroad.

- **National Crime Agency (NCA)**

Gill Tully and Sue Pope visited the NCA at Warrington on 18 June 2014, meeting representatives of the Interpol and SIRENE bureaus and the UK-Prum DNA and fingerprint Project. The process of validating European Arrest Warrants was discussed. The approach to scene to scene DNA matches uses a post search sift rather than pre-search limitations. Issues arise with partial matches to SGM reference samples that can no longer be upgraded since the S and Marper ruling has led to destruction of the stored samples.

ANNEX I

UIPDE & UKPFE Member State Case Studies

With the financial support of the Prevention of and Fight against Crime Programme

The following case studies have been provided by Member States through the UIPDE and UKPFE project as part of the research conducted by the SCJS research team.

Country	Year	Crime Type	Description of Case
Austria	2015	Murder (Multiple Homicides)	On 21th May 2015 a after a double homicide and robbery case is committed on an old and not wealthy married couple of pensioners in Vienna from one offender. The situation on crime scene showed a fully unnecessary execution of the old couple. One of the death bodies was additionally unclothed by the offender and described with latin words. Less valuables objects are partial are stolen but also more valuable items are left from offender on crime scene however the offender stay there for several hours beside of the death bodies. Obviously the offender likes primarily to kill his victims which have not any relationship to the killer. Our profilers are assumes from beginning, that the crime was committed by a minimum potential serial killer. After finalization of crime scene work and DNA analyses we got DNA profiles from the offender which we loaded in national DNA Database with No Hit result on 29th May 2015 noon. With the following fully automated Prüm searches starting minutes after this national search we have with the Austrian crime scene stains from the offender a Hit to an reference profile, stored in NL and additionally to an open stain stored in Germany. After immediate done forensic confirmation we start on afternoon of same day the 2nd step request for providing the background information to Netherlands and Germany. On Tuesday 2nd June 2015 we got all needed information from NL and DE. The NL reference profile sprang from a polish offender. He was sampled and stored in the NL after committed grievous bodily harm in 2011. The German open stain profile was secured in Germany in January 2015 after a burglar case in a grocery. With received fingerprints from the offender we have further Prüm AFIS person hits in Netherland, Poland and Germany (registration in Germany was done without DNA). Afterwards and with knowledge that the whereabouts of the offender are not known in all concerned states, we could start with his personal data, pictures and fingerprints at 3rd of June a worldwide arrest request. We start also actions by our target wanted person unit with electronically surveillance measures and additional with a public wanted person action by publication of his mug shots in mass media (TV, Internet and print media). With the actions of target wanted persons unit we could locate and arrest the offender on 08th of Junie 2015 in Düsseldorf / Germany on a Railway station. He tried to leave from Germany upon his arrest. With first results of investigations - he is beside of by stain confirmed crimes of him, strongly suspected to kill with same modus a person in Sweden. Update on case subsequently provided: The identified polish offender was extradited last week from Germany to Austria and is presently in investigative court custody in Vienna. In our first interviews he made immediate a comprehensive confession to the crimes he was suspicious.

			Beside of the double homicide and robbery committed on the old couple in Vienna, he give also a detailed confession with details to a murder case committed from him four weeks before in Goteborg, Sweden. During his arresting in Germany, he had the key of the stolen car from the Swedish victim with him. He has also admitted to an attempted homicide after a shop lifting in Salzburg, Austria in 2012. See attached some actual press release after first interviews with him. This offender has also raped the dying old lady in Vienna. However of his seemed mental disease and his joy by torture and killing of his victims, he know exactly at any time what he have done on crime scene and told us in interviews in a very detailed form his modus operandi by each crime. His testify covers exactly the perceptions of our crime scene work and investigations. We try now, to reconstruct the movements of this offender in the last years through Europe and will send his DNA profile with classical search requests now additional also to countries, which are presently not Prüm operative. It seems that he stay several years also in UK. It would be very surprising for us if he have not committed there serious crimes again. We are quite sure that he has committed much more crimes and perhaps also additional homicides that we could prove presently. I am absolutely sure that with his possible Prüm DNA hit identification and afterwards possible arresting we are able to prevent further murder cases and other crimes in Europe.
Czech Republic	2005 - 2013	1) Burglary 2) Murder 3) Robbery	Example 1: As an example we can mention a group of offenders operating on the territory of the Czech Republic in 2013. There were matches with DNA profiles processed in Slovak Republic. Afterwards Police of the Czech Republic merged 4 different criminal cases into one (burglary to jewelleries and some petrol stations and criminal damage on cars - firing, car-thefts in the second hands) which were investigated separately in both countries. Example 2: The genetic material was inserted into the Czech national DNA database during the investigation the crime of murder in 2011, the investigation was conducted against a particular offender who fled abroad. Genetic material was obtained from a cigarette butt in an ashtray in an apartment where a crime was committed. By comparing with national DNA database of Austria in 2014, it was found that the same profile is processed in Austria. Afterwards Criminal justice in Austria was contacted and asked to provide a suspect for criminal prosecution to the Czech Republic via legal assistance in criminal matters. Example 3: DNA profile was inserted into the Czech national DNA database in 2005 during the investigation the crime of robbery. Comparing the national DNA database with Austria in 2014 was detected specific person. Austrian side were asked a current photograph and other personal data via SPOC's.

Finland	Not Specified	Burglary (Multiple offences)	The biggest success story was presented in the DNA Prüm end seminar on May 6-7th, 2015 at Europol and will be available in Europol Platform for Experts shortly. In a nutshell, thanks to Prüm DNA match (4 cases), a perpetrator was identified, arrested and later found guilty in 50 aggravated thefts and 14 aggravated theft attempts (house burglaries). He had made 12 visits to Finland using different identities. The linking of the offences had been made by the police by using DNA matches, shoeprints, modus operandi and telecommunication monitoring data. He was imprisoned for 4 years in 2015. It appeared the same perpetrator was known in Austria, too, and did match in two crime stains in Sweden as well. The Austrian prosecutor is aware of the current status. There are some minor success stories, convictions based on Prüm matches related to aggravated drugs offence and aggravated thefts, too. The second biggest case where the identifying of the perpetrator was based on Prüm DNA match (26 burglaries) will be in court earliest late in summer 2015. In general, it is difficult to follow a case until the end as the information is not normally updated in police files after the case has been handed over to the judicial authorities.
Netherlands	1)1994 2)1998 3)2012 4)2014 5)2013		Example 1: In 1994 a 72 year old lady was killed in the town of Heerlen (near the German border) in the NetherlandsAt that time no suspect could be identified. When the Netherlands started to exchange DNA-profiles with Germany in 2008, a match with a person was found in the German DNA-database. The person proved to be a German citizen and hence could not be extradited to the Netherlands. So the case was handed over to Germany and the person was convicted in Germany in 2009Example 2: In 1998 a 19 year old woman was raped in the Netherlands. At that time no suspect could be identified. In 2010 there was a match with a person in the French DNA-database. The person was a citizen of Bosnia but no place of residence was known so a European arrest warrant was issued. In 2011 the person was arrested in Croatia, extradited to and convicted in the Netherlands.Example 3: In 2012 a jewellery shop was robbed by 3 persons in the city of The Hague in the Netherlands and one of the employees was seriously maltreated. DNA-profiles of 2 of the robbers were found at the crime scene. There was no match in the Dutch DNA-database but during the night 2 matches were found in the DNA-database of Lithuania with citizens of Lithuania. No place of residence was known for these persons so a European arrest warrant was issued.Example 4: In 2014 one person was arrested in Lithuania and extradited to the Netherlands. The other person was arrested in the UK and also extradited to the Netherlands. Both persons are in jail now waiting for their trial.Example 5: In the following link you will see the result of a very interesting Prüm match: http://www.dutchnews.nl/news/archives/2013/10/baby_boy_abandoned_in_roermond.php. Together with a new born boy which was abandoned in the Netherlands a DNA-profile of his mother was found. Her profile was included as a stain in the Dutch DNA-database because abandoning a child is punishable by a 4.5 year jail term. Hence her profile was sent to all operational Prüm countries and a match with a stain was obtained in the German DNA-database. This stain (just like in the Netherlands) originated from the mother of another abandoned child proving that both abandoned babies have the same

			(still unknown) mother.
Poland	2014	1) Burglary 2) Murder	DNA exchange with other MS has been very useful in a variety of different crimes and criminal investigations. Recently there was a case involving an OCG from Poland who travelled around Europe and were blowing up ATM machines to steal the contents. These attacks happened in Germany, Denmark, Sweden and Holland. While the case is still ongoing, investigators from these countries used the Prüm DNA system to identify the criminals by markers left at the crime scenes. In another case a murder investigation involving a Polish national in Austria yielded no results in both counties, however when this individual was arrested in Germany for an unrelated crime his DNA was collected and he was identified as the prime suspect in the Austria murder case.
Slovenia	2003	Rape	SUBJECT: RAPE IN THE VICINITY OF KOPER DNA PRÜM HIT, SLOVENIA (trace) – SPAIN (person) This case involves a rape, which was committed in 2003 in a cruel and extremely humiliating manner against a young girl in the vicinity of a small village near Koper. A DNA trace was preserved at the scene of the rape. The preserved trace was biological and it was collected from a cigarette butt, which was found at the scene of the criminal offence. At the beginning of the investigation, a suspect was arrested on the basis of police information and he even confessed to the rape. Later it was established that the suspect's DNA and the DNA preserved at the scene of the criminal offence didn't match, therefore the suspect was released. In the meantime, the unidentified DNA profile from the scene of the criminal offence of rape was sent to all countries via INTERPOL. At the time, INTERPOL informed us about a DNA hit between Portugal and Slovenia, which in the end confirmed the matching of the two DNA profiles, however this was a trace-trace hit. Also the case in Portugal involved the same criminal offence, i.e. rape. The Prüm hit occurred in 2007 during an automatic exchange of DNA profiles on the basis of the Prüm Treaty between Slovenia and Spain, and in this case the Spaniards had a DNA profile of a person. Since there was a likelihood that the suspect was still on the Slovenian territory and given the fact that all legal conditions (principle of availability) for the use of the tool called the Swedish Initiative were met, we decided to use this tool for this case. This was also the first example of the use of these two new tools at the same time (the Prüm Treaty and the Swedish Initiative). Spanish law enforcement authorities sent us a reply with necessary information regarding the Prüm hit. The reply contained several names of the person (aliases), because the person's identity wasn't established at that time.

			The most important part was the acquisition of identification material (photo and fingerprints) of the person, allegedly belonging to a citizen of Romania. In this regard, we immediately informed our competent authorities in charge of the case and at the same time we sent an urgent request to Romania via INTERPOL for the confirmation of his identity. All communication was carried out by the use of the Swedish Initiative tool. Interpol Romania confirmed the identity of the person and all the required information. All provided pieces of information were sent to our competent investigative authorities, who immediately provided for the issuance of a national alert for the person and later on the court issued an order for an alert also at the international level. As a consequence of all established facts, the court issued a European arrest warrant on the basis of which the wanted person was within three days arrested in Seville, Spain and extradited to Slovenia, where he is currently serving his 10-year prison sentence.
Cyprus	2012 - 2013	Burglary	On 18/11/2012 a house burglary took place in Nicosia. The intruders managed to stole a complete safety box 40cm x 50cm. Its contents (jewellery) reached a total price of more than 260,000euro. The processing of the crime scene revealed among other exhibits a set of latent fingerprints. The case was then considered by the CID investigators as a very serious one. Immediate assistance was asked by our laboratory. The prints found were initially considered to be connected to the intruders. The location that the prints were found matched the testimonies of the neighbours concerning the escape route of the suspect. The suspect jumped from a 3 meter wall to leave from the crime scene. Further assistance by our laboratory was considered to be vital for the cases final outcome.The fingerprints found were compared with those of people who had legal access in the residence. The prints did not match any of elimination prints. The fact that the prints did not match the elimination prints secured the initial assessment of the crime scene investigators. Next step was the crime scene prints to be loaded on our AFIS. The search in the local AFIS database produced no match.Next step was to submit the latent prints to the PRUM database. The tool called PRUM was at the early beginning of its implementation and not all of the police investigators were familiar with this alternative. The print was then loaded to all of the active PRUM fingerprint members. A hit was obtained with the Slovak Republic. Our laboratory immediately after the HIT prepared all the necessary paperwork. The police investigators were informed about the positive outcome of the case. The paperwork was sent on 27/11/2012 to European Union and International Police Cooperation Directorate which is the respective international police cooperation unit. Next step was to wait for the arrival of the EUROPOLs Sienna message containing the relative data of the suspect.The message received from Sienna on 28/11/2012 informed the Police authorities in Cyprus that the fingerprints belong to a Romanian national including all of his biographic data and photos. The message also stated that the Romanian national was fingerprinted on 28.9.2002 in Austria (Slovakia received the fingerprints via Interpol) and suggested that we should get in

			contact with the Austrian authorities. The message was forwarded to the police investigators.The police investigators then proceeded to the district court where they issued an arrest warrant for the Romanian suspect. All of his personal details were loaded on the stop list database. Following our request, on 07/12/12 our authorities were informed that the Romanian national was noticed in SIS with an arrest warrant since 22.08.2006 issued by the office of the public prosecutor at the criminal court in Vienna. The message also stated that because of burglaries a national arrest warrant was issued from 21.03.2012 issued by the office of the public prosecutor at the criminal court in Vienna.In April 2013 the suspect was arrested in Paphos. On 16/04/2013 the suspect was interrogated and fingerprinted by the Nicosia CID. His fingerprints were forwarded to our laboratory and confirmed our initial findings.The case was fully detected. Four other suspects were charged with engaging and planning the burglary. Cyprus Police extradited the Romanian national to Austria.ConclusionsThe following departments took part:-F.I.L-Nicosia district CID-European Union and International Police Cooperation Directorate-District courtThere is a need of a coordinator to be assigned in order to manage a Prüm Hit from the beginning until the end. The role of the coordinator can be expanded from strictly organising procedures to revising all current procedures, developing strategy to deliver a more efficient and effective handling of a case, establish a network between all the involved departments and establishing a framework of the overall handling. Contact points should be assigned to each department involved in order for them to develop expertise and to deliver immediate output as soon as a Prüm Hit occurs. Contact points and the coordinator can meet and exchange ideas from time to time with a view of delivering excellence. All relative data collected during the meetings will be available to all relative EU bodies if it is necessary. The Prüm Hit could be delivered in a relatively quick response time. The next step of receiving the remaining biographic data must be revised in order to be transmitted sooner than the current time taken. More than one countries may be involved. The case study involved more than one countries. The exchange of data request better coordination. The Prüm Hit may affect other country as well (travelling offenders). Suspect's data may be found in other database (SIS, Interpol). Better utilisation of the different databases. Need for decision to be taken to extradite a suspect.
The Netherlands		Robbery, stabbing, shooting False money Burglary Unidentified Body	Officers were called to reports of a robbery, a stabbing and a potential shooting. Witnesses reported a car driving away with a French number plate. The car was later found and latents collected from the scene were sent to Interpol for searching but no reply was ever received. Once live with Prüm, the latent was searched against the French database and a hit was returned. Case 1, False Money At a traffic stop the police find 3 million euro of false 500 euro bills where a number of suspects are arrested. The money is processed and one of the latents is from the fingerprints of one suspect who is identified. Other latents on the money are searched through Prüm and multiple hits come back from Germany, Austria and Lithuania.

		Robbery Street Robbery	Case 2, Burglary in Garden Sheds Multiple latents are found in a garden shed, where it seemed that somebody broke in and lived there for some time. Papers are found with German notes and a train ticket from Berlin to Amsterdam is also found. Latents deliver no match in the systems of the Netherlands, however, Prüm searches deliver hits from Germany and Lithuania. Case 3, Unidentified Body An unknown deceased man is found on a bench in a park in Amsterdam with no identity papers. Searches on national databases (criminal and alien) do not result in a match so Prüm searches are initiated and result in a match in Germany and Lithuania. The family is subsequently informed. Case 4, Robbery A dealer of expensive watches from Germany has contact with a potential buyer in the Netherlands. The dealer agrees to come to Holland with expensive watches and meet in a restaurant. Whilst showing the buyer the watches they are snatched by the buyer and he takes off. The dealer tries to stop the car of the thief but fails. In a bag left by the thief a package of false 500 Euro bills are found. Latents are found on the bills and searched in the national criminal AFIS, but no Match is found. Following a Prüm search, a hit in Spain with a man from former Yugoslavia is obtained. Case 5, Unidentified Body A victim of shooting is known in the Netherlands but there is doubt about his true identity. He had used a car with French license plates so a search in Prüm is conducted and delivers a hit in France with other personal data. Case 6, Street Robbery A victim is approached by 4 Romanians who put a "fake" gold necklace on the victim without asking. The suspects drive in a car with German number plates. Then a suspect tries to steal the (real gold) necklace of the victim by pulling it of her neck while driving away with the vehicle. The victim is dragged along for several meters. The MO and the description of the group match multiple incidents through Europe using a car with the same type of number plate but only one suspect is known. The car is then found in Amsterdam and latents are found on papers in the car. Latents have no hit in the National Criminal database so Prüm searches are initiated and they hit in Germany.

Czech Republic	2014 - 2015	Murder	July 2014: Parts of human body were discovered in two districts of Prague. A torso of a woman's body (trunk and both arms) was found in the building for sorting garbage in Prague 10. In Prague 3 the remainder of her body (head and the both legs) was found in another building for sorting garbage. Fingerprints were taken by an expert from the Criminal police and Investigation Service unit of Prague 4 (central criminal unit for Prague area). He performed AFIS searches with negative results. Subsequently, Criminal Police and Investigation Service Unit of Prague 4 made a request to the ICP for a search against the Prüm system. The woman's fingerprints were added to the national AFIS and a search was made of all 12 countries that were operational at the time with ICP. A positive hit was received from Germany. This was passed back to Criminal police and Investigation Service Unit of Prague 4.August 2014: Criminal Police and Investigation Service Unit of Prague 4 made a request to the Police Presidium, Department of International Police Cooperation for additional information from Germany. The following day the Police Presidium, Department of International Police Cooperation received additional information from Germany. The corpse of woman's body was from Ukraine living at the time in Prague with her Ukraine friend.After a short investigation, a perpetrator of the brutal murder was found. It turned out to be her friend mentioned above. He was charged with a murder at the beginning of December 2014. We expect the case will be tried by court in the beginning of March 2015.

Draft legislation for the purposes of Council Decision 2008/615/JHA and Council Framework Decision 2009/905/JHA[1]

PART 1

GENERAL

Interpretation

1. In these [Regulations]—

"convicted" includes—

(a) in England and Wales, the circumstances covered by section 65B of the Police and Criminal Evidence Act 1984 Act; and

(b) in Northern Ireland, the circumstances covered by article 53B of the Police and Criminal Evidence (Northern Ireland) Order 1989[2];

"dactyloscopic data" means any image of a fingerprint or palm print, including an image of a latent fingerprint or palm print, and including templates of such images;

"DNA-profile" has the meaning given by section 65 of the Police and Criminal Evidence Act 1984;

"forensic service provider" means any person that carries out any laboratory activity at the request of a person responsible for the prevention, detection or investigation of criminal offences;

"laboratory activity" means any measure taken in a laboratory when locating and recovering traces of DNA or dactyloscopic data on items, as well as developing,

[1] As noted in the Business and Implementation Case, there may also need to be further legislation or amendments to this draft legislation to fully capture these safeguards and forensic service provider requirements in relation to Northern Ireland and Scotland.

[2] Not yet commenced.

analysing and interpreting forensic evidence, with a view to providing expert opinions or exchanging forensic evidence with another member State;

“latent” means any fingerprint or palm print that through processing has been made visible for the purpose of creating an image;

“loci” means any set of identification characteristics of the non-coding part of an analysed human DNA sample, being the particular molecular structure at the various DNA locations;

“non-coding part of an analysed human DNA sample” means chromosome regions not genetically expressed, being those regions not known to provide for any functional properties of an organism;

“personal data” has the meaning given by section 1 of the Data Protection Act 1998;

“recordable offence” has the meaning—

(a) in England and Wales, given by section 118 of the Police and Criminal Evidence Act 1984;

(b) in Northern Ireland, given by article 2 of the Police and Criminal Evidence (Northern Ireland) Order 1989;

“reference DNA-profile” means any DNA-profile of an identified person;

“result of a laboratory activity” means any analytical output and any directly associated interpretation of such output;

“UKAS” means the United Kingdom Accreditation Service within the meaning of regulation 2(1) of the Accreditation Regulations 2009;

“unidentified DNA-profile” means any DNA-profile collected during the investigation of a criminal offence and belonging to a person not yet identified; and

“Union accredited forensic service provider” means any forensic service provider in any other member State accredited in accordance with Article 4 of Council Framework Decision 2009/905/JHA of 30 November 2009 on Accreditation of forensic service providers carrying out laboratory activities.

PART 2

DATA PROTECTION UNDER COUNCIL DECISION 2008/615/JHA

Scope of searches under Council Decision 2008/615/JHA

2. When, in accordance with Articles 3, 4 or 9 of Council Decision 2008/615/JHA, a member State searches or compares any DNA-profile or dactyloscopic data it holds against DNA-profiles or dactyloscopic data held by the United Kingdom, the national unit must ensure that those searches or comparisons are only against —

(a) unidentified DNA-profiles;

(b) reference DNA-profiles relating to persons who have been convicted of a recordable offence; and

(c) dactyloscopic data relating to persons who have been convicted of a recordable offence.

Provision of personal data following a DNA-profile match

3.—(1) Subject to paragraphs (2) to (4), where, pursuant to a search or comparison made by a member State under Articles 3 or 4 of Council Decision 2008/615/JHA, a match is shown between any DNA-profile held by that member State and any DNA-profile held by the United Kingdom, the national unit may provide the personal data it holds relating to the matched DNA-profile to the member State that made the search or comparison.

(2) The national unit must not provide the personal data where—

(a) the member State that made the search or comparison has not requested the personal data relating to the matched DNA-profile;

(b) the matched DNA-profile does not include ten or more matching loci;

(c) the personal data relates to a person aged under 18, unless the request for the personal data is received by the national unit following a formal request for mutual legal assistance; or

(d) subject to paragraphs (3) and (4), both the DNA-profile held by the member State and the DNA-profile held by the United Kingdom are reference DNA-profiles.

(3) In the circumstances set out in paragraph 2(d), the national unit may, unless one or more of paragraphs 2(a) to (c) applies, request that the member State

requesting the personal data provides dactyloscopic data for the person to whom the reference DNA-profile relates.

(4) Where—

(a) the member State requesting the personal data provides dactyloscopic data in response to a request under paragraph (3); and

(b) there is a match with dactyloscopic data held by the United Kingdom;

the national unit may, subject to paragraph (2)(c), provide the personal data it holds relating to the matched dactyloscopic data.

Provision of personal data following a dactyloscopic data match

4.—(1) Subject to paragraph (2), where, pursuant to a search made by a member State under Article 9 of Council Decision 2008/615/JHA, a match is shown between any dactyloscopic data held by that member State and any dactyloscopic data held by the United Kingdom, the national unit may provide the personal data it holds relating to the matched dactyloscopic data to the member State that made the search.

(2) The national unit must not provide the personal data it holds relating to the matched dactyloscopic data to the member State that made the search or comparison where—

(a) the member State that made the search has not requested the personal data relating to the matched dactyloscopic data; or

(b) the personal data relates to a person aged under 18, unless the request for the personal data is received by the national unit following a formal request for mutual legal assistance.

PART 3

ACCREDITATION OF FORENSIC SERVICE PROVIDERS

Scope of provisions relating to forensic providers

5.—(1) This Part applies to any laboratory activity resulting in:

(a) a DNA-profile; or

(b) dactyloscopic data.

(2) Nothing in this Part affects rules of evidence.

Accreditation

6. Any forensic service provider carrying out a laboratory activity must be accredited by UKAS as complying with BS EN ISO/IEC 17025:2005.

Recognition of results

7. A person responsible for the prevention, detection, or investigation of criminal offences must recognise the result of a laboratory activity provided by a Union-accredited forensic service provider as being equally reliable as the result of a laboratory activity provided by a forensic service provider accredited in accordance with Regulation 6.

Enforcement

8.—(1) If the Secretary of State becomes aware that a person has not complied with its duties under this Part, the Secretary of State may, by notice to that person, specify—

(a) measures that the person must take to ensure that that person complies with this Part; and .

(b) the deadline by which those measures must be taken.

(2) The Secretary of State must consider any representations about the notice received from the person to whom the notice is addressed, and may amend or withdraw the notice.

(3) If the specified measures have not been taken by the specified deadline, the Secretary of State may apply to the High Court for an order requiring the person to comply with the notice or otherwise carry out its duties under this Part.

Guidance

9. The Secretary of State may give guidance to a person responsible for the prevention, detection or investigation of criminal offences with respect to the practical implementation of this Part, and a person to whom such guidance is given must have regard to it.

ISBN 978-1-4741-2537-6