IPV OPERATIONS MANUAL

v3.1.1

1. Table of Contents

2. Purpose

1. The purpose of this document is to give detail to Identity Providers for providing identity-proofing capabilities in line with GPG 44 & 45 for the purposes of being a Certified Company for GOV.UK Verify. This SHOULD be read in conjunction with the other documents provided within that framework.

2. This document contains both requirements and guidance. The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (https://www.ietf.org/rfc/rfc2119.txt)

3. This document will be used as a controlling document by the certification body in order to determine whether the IDP has the capabilities to deliver identity-proofing services for GDS.

3. Identity Management

3.1. Registration

4. The IDP SHALL allow Users to register for a digital identity. The information needed is dependent on the target Identity Level required at the time of registration. Where the User has been directed to the IDP from the Identity Assurance Hub, the target Level of Assurance will be included in the request to the IDP therefore the IDP shall be able to determine the minimum Identity Level required.

3.1.1. Common registration requirements

5. The IDP SHALL require the User to provide an email address. The IDP SHALL only have one active account that uses that email address. The IDP SHALL confirm that the email address is under the control of the User (see Identity review (including revalidation)). The Evidence Details from the Identity Evidence SHALL be retained for future reference.

3.1.2. Specific registration requirements for each identity level

Identity Level	Registration Requirements
1	▪ The IDP SHALL require the User to declare their Claimed Identity or require the User to confirm the Claimed Identity where the Claimed Identity has been captured through a process that doesn’t require the User to provide such a declaration during registration. ▪ The Personal Name SHALL be the official name of the User. The IDP may ask for a name by which they want to be known as by the IDP. ▪ The IDP SHALL allow the User to declare their gender however it is not mandatory for the User to provide it. ▪ The IDP SHOULD capture telephone number for customer service purposes and counter identity fraud checks, although this is a decision for the IDP. ▪ Once the User has begun the identity proofing process (e.g. entering evidence, begun KBV) then the IDP SHALL only allow the User to pause and resume the process if they have successfully setup an appropriate credential (as set out in GPG 44) or the IDP issues a token via a channel that is known to belong to the Claimed Identity (not the User) which is used in conjunction with at least one other authentication factor. ▪ The IDP SHALL NOT inundate the user with messages in a manner that leads to message

	fatigue and desensitises them to phishing scams.
2	**Requirements for Level 1 plus the following:** ▪ The Personal Name SHALL be the official name of the User, aliases are not permitted.
3 & 4	**Requirements for Level 2 plus the following:** ▪ [redacted]

Table 1 Registration Requirements

3.1.3. Personal Details changed over the proofing period

6. The IDP SHALL ask the User to declare whether their personal details have changed over the period required by the proofing process (the Activity History length) except where this may contravene the Users's rights under section 7 under the Equality Act 2010.

7. Where the User declares to the IDP that there has been a change in their Personal Details the IDP SHALL gather those Personal Details from the User and attempt to Validate these changes.

8. The IDP SHALL attempt to gather evidence of the change of Personal Details from the User and the IDP SHALL Validate that evidence as per the requirements of GPG 45 and this document. Where this is not possible or practical the IDP SHALL confirm the changed Personal Details are known to an Authoritative Source (such as Data Aggregators).

3.2. Identity Data

3.2.1. Address

9. The IDP SHALL ensure the User provides a valid UK postcode where the address has been assigned a UK postcode. The IDP SHALL ensure that the postcode of a UK address is consistent with the address given, i.e. the User can not provide the postcode of an unrelated address. Where the User address is automatically, or semi-automatically, populated from a dataset (e.g. from a picker using PAF) and that dataset contains the UPRN (for a UK address) then the UPRN SHALL also be included in the Identity Assertion.

10. The IDP SHOULD be aware that a User may have multiple current addresses (e.g. where they live in different places during the week and weekends), the IDP SHALL encourage the User to provide at least the address that is related to their Identity Evidence, the IDP SHOULD collect all valid current addresses for the User, otherwise the proofing or matching process may be unsuccessful.

3.2.2. Names

11. Where the proofing or registration process requires the User's official name this means the name by which they are identified in official

records such as a register for births, marriages or civil partnership; or by official or legal documents that enable them to be known under that name, e.g. decree absolute, final order and deed of change of name (aka 'deed poll').

12. The IDP SHALL ensure that first name, surname and any middle names can consistently be identified from the data it has stored.

3.2.3. Dates

13. The IDP SHALL ensure that all dates both provided by the User (including date of birth, issue date, expiry date) and those generated by their own systems/data are valid dates for the given month and year (e.g. not 30/02/2011).

3.2.4. Historical data

14. Where the User has provided historical details for name, address and date of birth, the IDP SHALL retain these for at least 5 years within the User record in addition to the current details. The IDP may retain historical values for longer as long as this in line with legislation, other statutory requirements that apply to them and the terms and conditions that were agreed to by the User.

15. Where gender changes the IDP SHALL only ever retain the current value within the User's record.

3.2.5. PID

16. The IDP SHALL generate a persistent identifier (PID) for each User on registration. [redacted]. The PID SHALL remain unchanged for the lifetime of the User's account. The PID shall only be used for interactions with the Identity Assurance Hub and the PID SHALL never be reused, e.g. the PID shall not be used as identifier in other relationships the IDP has, a new PID SHALL NOT match a PID that has been deleted.

3.2.6. Personal details in the identity assertion

17. A minimum set of personal data SHALL be provided by the IDP in the identity assertion. Identity assertions SHALL only be sent after a successful authentication.

18. The Personal Details collected through the proofing process that SHALL be included in the identity assertion are:
    - First name, surname and middle names
    - Date of birth
    - Gender
    - Address

19. Only Personal Details that have been demonstrated to be true through a proofing process can be marked as 'verified' in the identity assertion.

20. The identity assertion SHALL contain historical details (up to 3 years) for these attributes except for Gender (which SHALL only ever contain the current value) where the IDP has collected such data.

3.3. Maintaining Accurate Identity Data

3.3.1. Updating verified data

21. The IDP SHALL enable the User to update their records to reflect a change in the User's circumstances after successful proofing. The IDP SHALL take appropriate measures to ensure that when this occurs it is being done by the legitimate owner of the account. The measures may vary depending on the strength of the Credential used to authenticate the User to the service that allows the User to change their details and other risk factors (e.g. detection of malware).

3.3.2. Validating change in a verified personal name

22. Where the User informs the IDP that there has been a change in their Personal Name after successful proofing the IDP SHALL attempt to gather evidence of the change of Personal Name from the User. The IDP SHALL Validate the evidence as per the requirements of GPG 45. Where this is not possible or practical the IDP SHALL confirm the changed Personal Name is known to an Authoritative Source (such as Data Aggregators). Also see Conditions for an Identity Assertion.

3.3.3. Validating change in a verified date of birth

23. This is an unusual event (but not unheard of) so where the User informs the IDP that there has been a change in their date of birth after successful proofing the IDP SHALL gather evidence demonstrating the change of date of birth from the User. The IDP SHALL Validate the evidence as per the requirements of GPG 45 and this document.

3.3.4. Validating change in verified address

24. Where User informs the IDP that there has been a change in their address after successful proofing the IDP SHALL attempt to gather evidence of the change of address from the User. The IDP SHALL Validate the evidence as per the requirements of GPG 45. Where this is not possible or practical the IDP SHALL confirm the new address is known to an Authoritative Source (such as Data Aggregators). Also see Conditions for an Identity Assertion.

3.3.5. Validating change in identifiers

25. Where the User changes an identifier and that identifier is used by the IDP as an outbound channel (e.g. a mobile phone number) then the IDP ensure that the identifier is in the possession or control of the User. Where the identifier is an email address then the IDP SHALL ensure that the email address is in the possession or control of the User (see Common registration requirements).

3.3.6. Verifying the User in order to enable a change in verified data

26. The IDP SHALL have processes to ensure the User is the owner of the account, by one of the following:
    - physical or biometric comparison,
    - knowledge based verification (KBV),
    - authenticating the User with appropriate method(s) and credential(s) for the Level of Assurance (see Determining the Level of Assurance and GPG 44).

3.3.7. Representing changed details in the identity assertion

27. When the User updated their data only that data that has been Validated can be marked as verified in the identity assertion.

3.3.8. Counter identity fraud checks for changes in User data

28. When the User changes their data, the IDP SHALL perform the counter identity fraud checks required for the level of the identity. This SHOULD be limited to the checks that are appropriate to the data items that have changed; e.g. a change of name SHALL necessitate counter identity fraud checks that are related to names, change in address SHALL necessitate counter identity fraud checks that are related to address. Where this process discovers a Contra-indicator then the IDP SHALL record that Contra-indicator against the User record and review the guidance in this document on dealing with Contra-indicators.

3.4. Credentials and Authentication

3.4.1. Credential issuance

29. All Credentials issued by the IDP for the purpose of authenticating a User SHALL:
    - Only be sent to an address or via communication channel that the IDP knows to be in control of the User. This SHALL either be via the identifier, email address, address, telephone or other communication channel that has been confirmed as part of the proofing process or has been subjected to an equivalent process.
    - Static Secrets (See GPG 44) used as part of the Credential SHALL NOT be sent in plaintext via an online channel.
    - Meet the requirements of GPG 44 for the specific LOA required.

3.4.2. Recovery of lost credential

30. The IDP SHALL have a process to enable a User who has lost their Credential to regain access to their account. The IDP SHALL verify that the User is the owner of the account, [redacted] whether this be online, by telephone or in person.

3.4.3. Display last login

31. After a successful authentication the IDP SHALL display the time of the last successful login (with the IDP) to the User. Where possible the IDP SHOULD indicate whether the last successful login was from the same device currently being used by the User.

3.5. Deregistration

32. At any time the User may choose to leave the IDP, therefore the IDP SHALL allow a User to close their account. When the User chooses to do so the IDP SHALL suspend all Credentials issued to the User and prevent any further authentications and assertions using that account. The IDP may offer a reasonable cooling off period to the User before closing the account. The IDP SHALL have processes to ensure the User is the owner of the account, this SHALL be by either:
    - physical or biometric comparison.
    - KBV.
    - authenticating the User with appropriate method(s) and credential(s) for the Level of Assurance (see Determining the Level of Assurance and GPG 44).
    - communication with the User to confirm the account closure outside of the immediate session/service.

33. The IDP SHALL allow the User to register again in the future if the User chooses to do so, the re-registration of such a User is treated as a new User (i.e. they are subjected to the same registration and proofing including being issued a new unique PID).

3.6. Notifications When There are Changes to a User’s Account

34. The IDP SHALL notify the owner of the account that their details have been changed using contact details that were not changed by the User at that time. This includes where a User has requested to close their account.

35. Where the User changes all contact details held against the account in the same session then the IDP SHALL ensure they are the owner of the account by one of the following methods: a physical or biometric comparison, KBV.

36. The notification SHALL occur via a process that is outside of the immediate session/service that is allowing the User to change their details (e.g. via email, instant message, text, telephone, letter). The IDP SHALL include instructions on how to recover from an unauthorised change to their details in the notification.

3.7. Identity Repair

37. A User may have their identity compromised by a 3rd party that could either prevent the legitimate User registering with an IDP or cause an existing account to be suspended by the IDP. The IDP SHALL ensure

they have the capability to register a User where they have been the subject of identity theft whilst being able to prevent the 3rd party doing so. The IDP SHALL ensure they have the capability to recover a closed User account where the account was closed by a 3rd party.

4. Identity Evidence (IPV Element A)

4.1. Determining Whether Identity Evidence is Applicable

38. The Identity Evidence SHALL be evaluated against the criteria set out in GPG 45. It SHALL only achieve the score from GPG 45 where is meets all the required properties for that score.

39. [redacted]

40. Identity Evidence that is available in the public domain is not permissible.

4.2. Linking The Claimed Identity to the Identity Evidence

41. The IDP SHALL ensure that the Claimed Identity given during registration is the same individual identified by the Identity Evidence. The Personal Name of the Claimed Identity SHOULD match the Personal Name demonstrated by the Identity Evidence. Where the Personal Name from the Identity Evidence and the Claimed Identity differ then the IDP SHALL determine that they relate to the same individual, e.g. where the Claimed Identity forename is Bill and the Identity Evidence is William (i.e. they are matching synonyms).

42. The date of birth of the Claimed Identity must match the date of birth as demonstrated by that Identity Evidence. If the date of birth differs then the IDP SHALL ensure the Claimed Identity has the correct date of birth by either updating the Claimed Identity using the date of birth from **validated** Identity Evidence (see Validation) or requesting the User to correct it. However if the IDP believes the Identity Evidence to have a different date of birth (based on other information they have) then that Identity Evidence SHALL be void.

5. Validation (IPV Element B)

5.1. Applicability of Identity Evidence

43. Identity Evidence must be valid at the time of registration; therefore the IDP SHALL ensure that the Identity Evidence has not passed its expiry date [redacted]. Checks performed against the Issuing/Authoritative Source are likely to fail if the Identity Evidence is no longer valid.

5.2. Determining whether Identity Evidence is Genuine

5.2.1. Examination of the security features of a physical document

44. This chapter provides the specific requirements for validation of the physical Identity Evidence (e.g. physical documents) provided by the User in order to determine whether the Identity Evidence is **Genuine**.

45. The IDP capability to Validate identity documents will affect the determined level of identity assurance. The following table provides the personnel training and equipment capabilities that are required from an IDP in relation to the IPV Element B score required for Validation.

Score	Equipment Requirements	Training Level
1	▪ [redacted]	AWARE
2	▪ [redacted] **OR** ▪ [redacted]	BASIC
3	▪ [redacted] **OR** ▪ [redacted]	ADVANCED

	[redacted]	
4	▪ [redacted] **AND** ▪ [redacted]	ADVANCED

Table 2 Document Inspection Equipment and Training

46. Each of the training levels in the following table builds on the training of the previous level, e.g. to achieve BASIC level training the trainee SHALL have either previously completed a training programme for AWARE or that the training required for AWARE is also covered in the BASIC training programme.

Training Level	Training Requirements
AWARE	▪ [redacted]
BASIC	[redacted]
ADVANCED	[redacted]

	[redacted]

Table 3 Document Training Requirements

47. Reference material (not a definitive list)

- Prado *http://www.consilium.europa.eu/prado/en/prado-start-page.html*
- National Document Fraud Unit guidance on examining identity documents https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/536918/Guidance_on_examining_identity_documents_v._June_2016.pdf
- CPNI document verification http://www.cpni.gov.uk/documents/publications/2007/2007044-gpg_document_verification_guidance.pdf
- Catalogue of identity documents http://www.catalogueofcurrencies.com/en/identity-documents.html
- Security features guide http://www.catalogueofcurrencies.com/en/security-features-guide.html
- UK Photocard driving licence *http://www.consilium.europa.eu/prado/en/prado-documents/gbr/f/index.html*
- Passports
    - Introducing the new United Kingdom passport (2010) *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118767/introducing-new-passport.pdf*
    - Basic passport checks *https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118783/basic-passport-checks.pdf*

- Secure payment cards
    - American Express card security features https://secure.cmax.americanexpress.com/Internet/International/japa/SG_en/Merchant/PROSPECT/WorkingWithUs/AvoidingCardFraud/HowToCheckCardFaces/Files/Guide_to_checking_Card_Faces.pdf

5.2.2. Physical evidence containing cryptographically protected information

48. For physical documents that contain cryptographically protected information (e.g. RFID in passports, EMV Smartcard):

- Extract the embedded data from the Identity Evidence with a compatible reader. Where the information is protected from being read, e.g. secured using ICAO 9303 compliant basic or enhanced access control mechanism, provide the required access/decryption key, e.g. from the information in the Machine Readable Zone (MRZ) on a ICAO 9303 compliant passport. Where the cryptographic system requires a PIN the User SHALL enter it themselves.
- If the chip was successfully read then compare the retrieved information with the Personal Details and Evidence Details (where such details are held) on the evidence to ensure they are consistent.
- Confirm the digital signature is correct.
- Confirm the signing key is valid with the Issuing/Authoritative Source.
- Confirm the signing key is the correct key for the Identity Evidence with the Issuing/Authoritative Source (i.e. this is the correct key used by the issuer for this type of Identity Evidence).

5.2.3. Electronic evidence containing cryptographically protected information

49. For electronic Identity Evidence (e.g. PDF):

- Confirm the digital signature is correct.
- Confirm the signing key is valid with the Issuing/Authoritative Source.
- Confirm the signing key is the correct key for the Identity Evidence with the Issuing/Authoritative Source (i.e. this is the correct key used by the issuer of this Identity Evidence).

5.3. Checking if the Identity Evidence is Valid

50. Some forms of Identity Evidence include features such as check digits and specific identifier structures, the IDP SHOULD confirm the information provided is consistent with these features otherwise any check performed against the Issuing/Authoritative Source is likely to fail. The following are examples for some of the Identity Evidence:

51. DVLA Driver Number

The driver number assigned by DVLA is a compound identifier made from information about the driver and some DVLA specific information. It is constructed as follows:

- Characters 1 to 5 - first five letters of the surname; if the surname has fewer than five letters, the remaining spaces padded using the number 9, e.g. FOX99. Note: some names may have been amended by DVLA to improve uniqueness, e.g. MAC is shortened to MC.
- Character 6 - the decade from the year of birth, e.g. 7 for 1974.
- Characters 7 & 8 - the month taken from the date of birth. If the gender is female, a value of ‘5’ is added to character 7, e.g. a woman born in October (10) would have ‘60’ for these characters.
- Characters 9 & 10 - day of the month from the date of birth, e.g. 15 for 15/04/1982.
- Character 11 - the last digit from the year of birth, e.g. 4 for 1974.
- Characters 12 to 13 - the first two initials of the given names. Unused characters are usually padded with ‘9’ however to ensure uniqueness other numbers are sometimes used.
- Character 14 is usually padded with a ‘9’ however to ensure uniqueness other numbers are sometimes used.
- Characters 15 & 16 - security digits generated by DVLA.
- Characters 17 & 18 - issue number.

52. Issuer Identification Number Compliant with ISO/IEC 7812

ISO/IEC 7812 (e.g. bank & credit cards) is the international standard that specifies "a numbering system for the identification of issuers of cards that require an issuer identification number (IIN) to operate in international, interindustry and/or intra-industry interchange”. It is constructed as follows:

- Characters 1 to 6 - The issuer identifier number (IIN) as assigned by "ISO Register of Card Issuer Identification Numbers" (Character 1 is also the major industry identifier (MII) number as defined by ISO/IEC 7812).
- Characters 7 to second last (maximum of 12 digits) – Account number as given by the card issuer.
- Last digit - check digit calculated using the Luhn algorithm as defined in Annex B of ISO/IEC 7812-1.

53. To check if information is accurate the Personal Details and Evidence Details need to be confirmed as Valid by the Issuing/Authoritative Source. In practice this means the Personal Name, Address and/or DoB, at least one unique number (where the Identity Evidence has a unique number) and expiry date (where the Identity Evidence has an expiry date) from the Identity Evidence SHALL be confirmed by the

Issuing/Authoritative Source as being identical to their records. Identity Evidence can not be determined to be Valid from inspection of the Identity Evidence itself (see **Genuine**). The following are examples for some of the Identity Evidence:

54. ICAO 9303 Passport

ICAO 9303 is the international standard for Machine Readable Travel Documents (MRTDs) that includes electronic passports that are used worldwide. The information that is required for Validation is as follows:

- Passport number
- Code (issuing state)
- Given Name(s)
- Surname
- Date of birth
- Date of expiry
- Optionally: Date of issue
- Optionally: Place of birth
- Optionally: Authority
- Optionally: Type
- Optionally: Sex (the User SHALL NOT be mandated to provide this)

Note: Both the biographic data printed in the main section of the passport and the data in the Machine Readable Zone (MRZ) are valid representations of the identity information. However they may not be consistent with each other since the MRZ uses a limited character set that has been transliterated from the original language and only contains alphanumeric characters as required by the ICAO 9303 specification. No punctuation marks will be represented in the MRZ, these may be replaced by "<" or simply removed depending on the original language.

55. Directive 2006/126/EC compliant driving licence

Directive 2006/126/EC sets out the standard for driving licences issued by EU member states. To avoid translation and language issues the licence only uses numerical references to identify fields. The field numbers required for Validation is as follows:

- 5 (driver number)
- Country code of the issuing member state
- 1 (surname)
- 2 (given name)
- 3 (date and place of birth)
- 4a (issue date)
- 4b (expiry date)
- 4c (issuing authority)
- Optionally: 8 (address)

- Optionally: Issue number

5.4. Outcome of Validation

56. If the IDP is unable to Validate the Identity Evidence they SHALL record the failure against the User record. Where the process discovers a Contra-indicator then the IDP SHALL record that Contra-indicator against the User record and review the guidance in this document on dealing with Contra-indicators (see Contra-indicators).

6. Verification (IPV Element C)

6.1. Knowledge Based Verification

57. Knowledge Based Verification (KBV) uses information about the Claimed Identity that should be only known by them to verify that the User is indeed that Claimed Identity. This is usually achieved by challenging the User in a manner so that only the Claimed Identity could reasonably be expected to respond correctly.

6.1.1. KBV principles

58. There must be a sensible balance between achieving assurance that the User is the owner of the Claimed Identity and presenting an acceptable User journey. With this in mind the IDP SHALL follow a number of KBV principles:

59. Principle 1: Clarity. The KBV process SHALL be clear so that the User is able to understand and correctly respond:
    a. KBV process SHALL be relevant, sensible and proportionate.
    b. KBV process SHALL be carefully constructed as to be clear and obvious to the User what is being asked of them (e.g. where this a question such as “amount of last statement” could be misleading as the data may not represent the last statement the Claimed Identity had received due to latency in backend systems).
    c. There SHALL be an expectation that the owner of the Claimed Identity can reasonably be expected to be able to complete the KBV process.

60. Principle 2: Breadth. The KBV process SHOULD cover a wide range of information:
    a. KBV process SHOULD be based on a range of information and not reliant upon one single KBV source; where Data Aggregators are used then the IDP SHALL ensure that the KBV process do not relate to the same source.
    b. KBV process SHOULD cover different Evidence Categories; ideally where the User has only provided 2 forms of Identity Evidence then KBV process relating to the unused Evidence Category SHOULD be included.

61. Principle 3: Security. The KBV process SHALL protect the Claimed Identity from impersonation:
    a. The KBV process SHALL be constructed so that the loss or theft of a possession such as a wallet/ purse would not provide the required information to pass it.
    b. KBV data SHALL NOT be used where it is known, or likely, that it is in the public domain. Information in the public domain in this context means KBV data that can be accessed by someone other than the person to whom it relates either with or without a

degree of research or is contained within an open dataset or website.

c. Where the KBV process offers the User a selection of suggested answers (i.e. multiple choice) then all the answers SHALL be plausible and the correct answer SHOULD NOT be easily guessed.
d. KBV process SHALL be constructed so that it is unlikely that the answers can be drawn from information available in the public domain, including social networking sites and public registers.
e. The KBV process SHALL minimise the risk that it can be passed by a close family member or friend, however it is accepted that in some cases this might not be possible.
f. The KBV process SHALL ensure that where this includes multiple questions that one question doesn't effectively answer another; e.g. the IDP SHALL NOT ask "You took out a mortgage with A.Lender in April 2013, what is your monthly payment?" and "You took out a mortgage in April 2013, who was it with?" (the first question answers the second).
g. The KBV process SHALL ensure that where multiple possible answers are presented that they vary from user to user in a manner that makes it unlikely that the correct answer is predictable.
h. The KBV process SHALL ensure that answers have not previously been provided by the User elsewhere in the service; e.g. the IDP SHALL NOT ask "Which of these is your previous address?" where the User has already provided that address (either during registration or by the User later updating their account).
i. The KBV process SHALL NOT reveal personal information to the User that they have not already provided (e.g. "You have a joint account with J. Doe, which bank is this with?" where the relationship to J. Doe was not already provided by the User).

62. Principle 4: Sources. The IDP SHALL ensure that they are using suitable sources in the KBV process:
    a. In this context a source is considered to be the organisation that captures/generates the original data, not any intermediary, such as a Data Aggregator, that is used to gain access to that data.
    b. A source is considered to be an organisation in its entirety however where that organisation has within itself separate acceptance and proofing processes then data that originates from those separate processes can be considered as a separate source (e.g. bank account and mortgage from the same provider could count as different sources if the processes to obtaining them were separate).
    c. A source used for KBV must be independent from the User, e.g. KBV questions cannot be based on information already provided by the User.

d. Where the source of the KBV is the proofing organisation (e.g. a code or reference number) then they SHALL only use a delivery method that ensures it is delivered to the Claimed Identity (not the user).

6.1.2. Static and Dynamic Data

63. Data used for KBV that varies over time is considered to be ‘dynamic’. [redacted]

6.1.3. Shared Codes

64. Where an IDP uses a code as part of the KBV process it shall have sufficient randomness so that it would be difficult to guess. The code SHALL be created by a random number generator that follows Good Industry Practice. As a minimum the code SHALL be a length as shown in the following table.

Validity Period	Same case alpha	Mixed case alpha	Numeric only	Same case alphanumeric	Mixed case alphanumeric
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 4 Shared Code Length

6.1.4. KBV data

65. The degree of assurance that can be taken from the KBV process is linked to the quality and availability of the data used. The following describes how to consider the quality of the data. KBV data is only valid if it refers to an individual whose Personal Details match those of the Claimed Identity (also see Data Aggregators).

KBV Quality	Properties of KBV Data
Low	▪ KBV data SHALL be pertinent to the Claimed Identity. ▪ The KBV data cannot be obtained with ease, with or without a financial commitment. ▪ The source of the KBV data protects the integrity of the KBV data. ▪ The KBV data is not known, or likely, to be in the public domain including any public register.
Medium	**Requirements for “Low” plus the following**: ▪ The source of the KBV data confirmed the Claimed Identity through a proofing process. ▪ The KBV data may be available to others, including relations and friends, but would require

	a financial commitment that would be a deterrent to others. ▪ The KBV data would require a time commitment to research that would noticeably delay an impostor's ability to provide the correct answer during the KBV process. ▪ The source of the KBV data protects the confidentiality of the KBV data. ▪ Where the KBV is a shared secret the delivery mechanism for the shared secret means that it can 'reasonably be assumed' to have been delivered into the possession of the Claimed Identity (not the User).
High	**Requirements for "Medium" plus the following**: ▪ The source of the KBV data confirmed the Claimed Identity in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2017. ▪ KBV data SHOULD NOT be known to others apart from the owner of the Claimed Identity (and immediate family). ▪ Someone other than the Claimed Identity (and immediate family) SHOULD NOT be able to obtain the KBV data without committing either a civil or criminal offence. ▪ The source of the KBV data have security practises that prevent unauthorised access, modification or generation of KBV data by insiders, either acting alone or with outside coercion. ▪ The source of the KBV data SHALL be subject to regulation by a statutory or an independent body. ▪ The source used for KBV SHALL be reliable and independent from the service providing the proofing (see Reliable and Independent Sources). ▪ Where the KBV is a shared secret the delivery mechanism for the shared secret ensured that it was delivered into the possession of the Claimed Identity. ▪ The KBV SHALL be 'dynamic'.

Table 5 KBV Quality

66. KBV data SHALL NOT be used where it is known, or likely, that it is in the public domain. In this context information in the public domain means that the KBV data can be accessed by another person either with or without a degree of research or financial commitment, or is contained within an open/public facing website.

6.1.5. KBV scoring

67. To ensure that there is a consistent KBV approach for demonstrating that the User has sufficient knowledge about the Claimed Identity the IDP SHALL follow the scoring model set out in this document.

68. The score is dependent on two factors, the KBV Quality and the method by which the response is elicited from the User. In this context "Unprompted" means a method where the response is not constrained or limited to a defined subset (e.g. free text entry) and "Prompted" means a method where the response is constrained or limited by the IDP to a set of values (e.g. multiple choice). The following table demonstrates the scoring profile for KBV.

KBV Quality	Unprompted Success	Unprompted Failure	Prompted Success	Prompted Failure
Low	[redacted]	[redacted]	[redacted]	[redacted]
Medium	[redacted]	[redacted]	[redacted]	[redacted]
High	[redacted]	[redacted]	[redacted]	[redacted]

Table 6 KBV Scoring

69. Users start the KBV process with a success score of [redacted] and failure score of [redacted]. Where a User correctly answers a KBV question their success score is incremented by the score as detailed above; where the User fails to correctly answer a KBV question their failure is decremented by the score as detailed above. The success and failure scores SHALL NOT be added together, they are distinctly separate counters.

6.1.6. Pausing, Resuming & Restarting KBV

70. Where the IDP allows the User to pause and resume the proofing process care shall be taken to ensure that they cannot use this feature to gather information relating to the Claimed Identity from the KBV process.

71. [redacted]

72. [redacted]

73. [redacted]

74. Where the IDP allows the User to pause and resume the KBV process then the IDP SHALL ensure it does not reveal to the User whether they have correctly answered any question until they have completed the whole KBV process.

75. The IDP SHALL only allow the User to pause and resume KBV [redacted].

76. If upon return the User fails to complete KBV then the IDP SHALL treat this in the same manner as a User failing KBV at the first attempt.

77. Whether the IDP needs to apply the pause & resume rules is dependent on whether the User exited or paused the process whilst the KBV process was being performed and by the time period elapsed between when the User paused and resumed the KBV process:

   a. If any KBV challenge has been displayed to the User then regardless of whether the User chooses to answer it or not the KBV process is deemed to have begun and the pause & resume requirements apply.
   b. If the User returns to complete KBV within [redacted] then this is considered to be a resumption of the process and the pause & resume requirements apply.
   c. If the User returns to complete KBV between [redacted] then this is considered to be a partial restart of the KBV process and paras 71, 73 and 74 still apply however all other conditions relating to KBV pausing, restarting and resuming are reset.
   d. If the User returns to complete KBV after [redacted]then this is treated as a restart for the purposes of KBV and all conditions are reset.

6.1.7. Other KBV considerations

78. The IDP MAY allow the User to skip a challenge. [redacted]. The IDP shall not allow the challenge to be used again in the current KBV process (including any pause & resume or partial restart activity). The IDP SHALL NOT allow a User to skip more than [redacted] challenges in total within the current KBV process (including any pause-resume and partial restart activity).

79. [redacted]

80. These two considerations are not mutually exclusive.

6.1.8. Passing and failing KBV

81. Unless an contra-indicator or other known risk implies otherwise, KBV is completed at the KBV Level as set out in the table below.

Identity Level	KBV Level
1	[redacted]
2	[redacted]
3	[redacted]
4	[redacted]

Table 7 KBV Level

82. The User is deemed to have passed KBV if they achieve the success total before achieving a failure total as defined in the table below. The User is deemed to have failed KBV if they achieve the failure total before achieving a success total as defined in the table below.

KBV Level	1st Attempt Success Total	1st Resume Success Total	2nd Resume Success Total	Failure Total
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 8 KBV Pass/Fail Scoring

6.2. Physical Comparison

83. The physical comparison step of verification requires the User to be verified by a visual confirmation that they appear to be the person to whom the Identity Evidence was issued. There are two methods by which this may be completed, a traditional in person/face-to-face process and a remote process (e.g. using a video/video streaming link). Below is a table of quality controls that SHALL be considered when performing either process.

Physical Verification Method	Quality controls
In person	▪ If a person is performing the comparison they SHALL have sufficiently good eyesight (when wearing any prescribed corrective lenses) to be able to accurately see the image/photo and the User. ▪ If a person is performing the comparison they SHALL have been trained in detecting impostors [redacted]

	▪ [redacted] ▪ Any electronic matching capability used SHALL have been independently assessed by a reliable and independent body as being able to demonstrate a high degree of accuracy in distinguishing between people of similar characteristics. ▪ Size and quality of the original image/photo SHALL be good enough for someone to be identified[redacted]
Remote	**Requirements for "in person" plus the following:** ▪ Where the image of the Identity Evidence has been captured through an electronic channel then the quality of the Identity Evidence image SHALL be at least[redacted]where the Identity Evidence constitutes [redacted] image and is in focus; [redacted]. ▪ The visual representation of the User SHALL be of sufficient quality [redacted] and be clearly recognisable. ▪ The IDP SHALL take sufficient procedural and technical measures to ensure that the visual representation of the User is of a real person and not a photo or other mock up.

Table 9 Physical Verification Quality Controls

6.3. Biometric Comparison

84. Biometric comparison requires the User to be verified by a biometric confirmation that they appear to be the person to whom the Identity Evidence was issued. [redacted] The capture of the biometric for comparison SHALL have sufficient measures to detect the spoofing of biometric identifiers.

6.4. Failing Verification

85. If the IDP is unable to Verify the User as the owner of the Identity they SHALL record the failure against the User record. Where the process produces a Contra-indicator then the IDP SHALL record that Contra-indicator against the User record and review the guidance in this

document on dealing with Contra-indicators before deciding whether to fail this IPV Element.

7. Counter Identity Fraud Checking (IPV Element D)

7.1. Counter Identity Fraud Checking

86. [redacted]

7.2. Failing Counter Identity Fraud Checks

87. If the IDP determines that the User has failed IPV due to information gained from the counter identity fraud checking process they SHALL record the failure against the User record. Where the process discovers a Contra-indicator then the IDP SHALL record that Contra-indicator against the User record and review the guidance in this document on dealing with Contra-indicators before deciding whether to fail this IPV Element.

8. Activity History (IPV Element E)

88. Activity History is derived from a process based on the following information and analysis:
    - Qualifying Activity Events
    - Quality of the Activity Events
    - Weighting of Activity Events
    - Activity History Profile

89. It is the combination of these things that indicates that the Claimed Identity has an existence over time.

8.1. Qualifying Activity Events

90. In order to determine Activity History there must be a collection of qualifying Activity Events to assess. To qualify, the Activity Event SHALL relate to an interaction between the Claimed Identity and a source of Activity Events. This can be in either direction, e.g. the Claimed Identity using the services of the source or the source initiating an interaction with the Claimed Identity including issuing something to the Claimed Identity, regular automated processes that can occur even if the Claimed Identity were inactive (such as standing charges) are not applicable.

91. Activity Event data is only valid if it refers to an individual whose Personal Details match those of the Claimed Identity, allowing for any changes in Claimed Identity that have occurred over the time period being assessed for the Activity History.

92. Qualifying Activity Events are usually demonstrated by a direct action performed by the Claimed Identity however some Activity Events may be derived where the data doesn't contain the actual Activity Event but that data could only be true if the Claimed Identity was active, [redacted]

93. In order to meet the Activity History requirements the IDP may extend the Activity History period to include more qualifying Activity Events. In such cases the Activity History assessment SHALL cover the period from the oldest Activity Event to the most recent.

94. [redacted]

8.2. Activity Event Quality

95. The degree of assurance that can be taken from the Activity History process is linked to the quality of the data used. Each Activity Event SHALL be measured against the quality criteria before assessment of the Activity History, however in practise the quality is likely to be determined by the source (generally a source tends to produce data of

the same quality). The following describes how to consider the quality of that data and attributes a Quality Score (QS) to each. In this context "source" is considered to be the organisation that captures/generates the original data [redacted] and not any intermediary, such as Data Aggregators, that is used to collate or access that data.

Quality	Score	Properties of Activity Event Quality
Low	1	▪ Data SHALL be pertinent to the Claimed Identity. ▪ The data source SHALL record accurate timestamps against the Activity Event. ▪ The data source SHALL protect the integrity of the Activity Event.
Medium	2	**Requirements for "Low" plus the following**: ▪ An individual could generate the Activity Events but it would require a financial commitment or a level of difficulty that would be a deterrent. ▪ The identity linked to the data within the data source was confirmed through an identity proofing process. ▪ The Activity Events are independently verifiable. ▪ The data source has a process for reporting and rectifying identity-related issues such as identity theft.
High	3	**Requirements for "Medium" plus the following**: ▪ The identity linked to the data within the data source was confirmed in a manner that complies with the identity checking requirements of The Money Laundering Regulations 2017. ▪ The data source SHALL have security practises that prevent unauthorised modification or generation of data by insiders, including acting alone or with outside coercion. ▪ The data source SHALL be subjected to regulation or audit by a statutory or an independent body.

Table 10 Activity Event Quality

8.3. Weighting of Activity Events

96. It has to be recognised that low quality events that have a long history are useful in assessing Activity History and high quality events that only have a short history may simply be the result of someone attempting to create a false identity. Therefore the Quality Score SHALL be weighted in relation to the length history available of the Claimed Identity from that source [redacted]

[redacted]

Weighting Condition	Weighting
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 11 Activity Event Weighting

97. The following table summarises how the quality and weighting combine to produce a score for the Activity Event.

		Longevity of Claimed Identity known by source					
			[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Activity Event Quality	L		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	M		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	H		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 12 Activity Event Scoring

8.4. Breadth of Activity Events

98. The Activity Event Package as described in GPG 45 requires a spread of Activity Events over multiple categories. [redacted] The following table demonstrates how the Activity Event Score, the Level of Identity and breadth of categories relate [redacted]

99.

Number of Evidence Categories (CML) required					
		Level of Identity			
		1	2	3	4
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 13 Breadth of Activity Events

100. The number of categories required is determined by the highest scoring Activity Event Score (AES) that occurs within the Activity History Profile for the required Level of Identity. [redacted]

[redacted]

8.5. Profiling Activity History

101. To achieve the Activity History criteria as defined by GPG 45 the IDP SHALL determine that the Activity Events meet the Activity Profile required for the level of identity. [redacted]

8.6. Activity Period Scoring

102. [redacted]

103. The minimum required Activity Period Total is calculated [redacted]

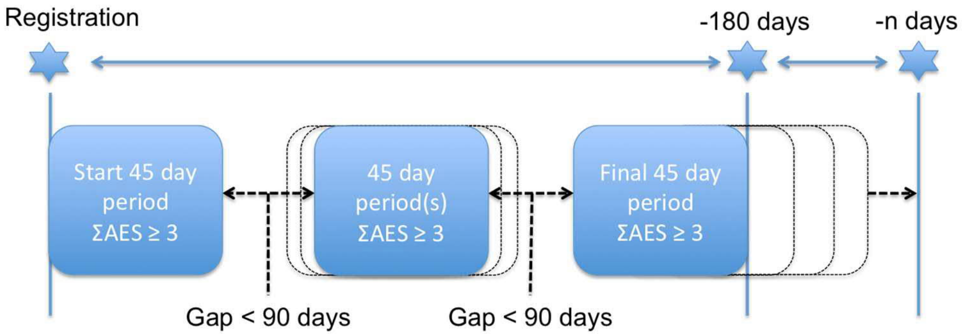
Identity Level	Activity Profile Score
1	N/A
2	[redacted]
3	[redacted]

Table 14 Activity Profile Scores

104. [redacted]

105. [redacted]

106. [redacted]


Registration
-180 days
-n days
Start 45 day period ΣAES ≥ 3
45 day period(s) ΣAES ≥ 3
Final 45 day period ΣAES ≥ 3
Gap < 90 days
Gap < 90 days

[redacted]

[redacted]

8.7. Failing Activity History

107. If the IDP is unable to determine the required Activity History they SHALL record the failure against the User record. Where the process produces a Contra-indicator then the IDP SHALL record that Contra-indicator against the User record and review the guidance in this document on dealing with Contra-indicators before deciding whether to fail this IPV Element.

9. External Sources

9.1. Data Aggregators

108. A Data Aggregator is an organisation involved in compiling information on individuals from various sources. For the purposes of IPV they SHALL also meet the criteria for being a reliable and independent source.

9.1.1. Matching records against those from a Data Aggregator

109. As Data Aggregators compile information from multiple sources there is no guarantee that all Personal Details from every source will match exactly to the Claimed Identity provided by the User on every single entry (e.g. there maybe keying/rekeying errors, OCR misreads, transpositions etc). The view of the dataset (of the Personal Details) taking into consideration the likelihood of the source having the correct details, predictable inconsistencies and weightings SHALL be considered the most likely representation of the actual Personal Details (e.g. most common version of the name given the likelihood of the sources collecting the official name and not synonyms).

110. When matching the Claimed Identity against such datasets the following rules SHALL apply:

Item	Matching Rules
Personal Name	▪ Matching is permitted to take into consideration known synonyms for given names (e.g. Bill & William). [redacted]
Dates (including Date of Birth)	[redacted]
Address	▪ Matching SHALL always match exactly on postcode (for a UK address that appears to have been assigned a postcode). ▪ Matching SHALL always match the main property identifier (e.g. House No. 1 Flat 1A matches House No.1 Flat A).

Table 15 Matching with Data Aggregators

9.1.2. Data Aggregators and KBV

111. Where KBV data is sourced through a Data Aggregator then the aggregator SHALL have a strong data handling process, ensuring compliance with Law, that the data is only supplied to appropriate organisations/persons and protect against unlawful and accidental disclosure. Protection of the confidentiality and integrity of this data is key to ensuring that KBV has value; if someone's KBV data is lost or stolen then that will fundamentally undermine its effectiveness in the IPV process.

9.1.3. Data Aggregators and Activity History

112. Where Activity Event data is sourced through a Data Aggregator then the aggregator SHALL have a strong data handling process, ensuring compliance with Law, that the Activity Event data is only supplied to appropriate organisations/persons and protect against unlawful and accidental disclosure. Protection of the integrity of this data is key to ensuring that Activity Events have value. If Activity Events can easily be falsified then that will fundamentally undermine their usefulness in the IPV process.

9.2. Reliable and Independent Sources

113. As part of the proofing process the IDP may check or collect various pieces of information from a reliable and independent source.

114. A source is considered to be reliable and independent where **all** of the following conditions are met:
    - Recognised as being a suitable source for the information being sought/checked within Good Industry Practice.
    - Demonstrate they can provide a dependable service.
    - Demonstrate that the staff and processes operate independently from those involved in the identity proofing processes within the IDP.

10. Contra-indicators

10.1. What makes a contra-indicator

115. Contra-indicators are essentially pieces of information that either contradict statements from the User or raise some doubt over whether the User is legitimate. Contra-indicators are discovered either during the proofing process or during the lifetime of the User's account, some arise from the Validation, Verification and Activity History steps but they are most commonly discovered during the counter identity fraud checking process.

116. The discovery of a contra-indicator does not necessarily mean that the User is not legitimate. Most contra-indicators will require further investigation in order to confirm they are not a false-negative. Some contra-indicators are warnings to the IDP that they may need to perform more stringent checks, e.g. the Claimed Identity has been the subject of identity theft and the IDP needs to ensure that the User is indeed the owner of the Claimed Identity and not an impostor.

10.2. Analysing a contra-indicator

117. During the proofing process a number of contra-indicators may be discovered. The IDP SHALL review the contra-indicators and make an assessment on whether they believe the User may be making a false claim to an identity. Where the IDP attempts to resolve a warning raised by a contra-indicator they should not disclose the exact nature of that contra-indicator to the User.

118. The IDP SHALL ensure that they have taken reasonable steps to determine whether a contra-indicator is false-positive. The Contra-indicator Table is a list of contra-indicators that the IDP may encounter and includes guidance on how to interpret and react to them. Each contra-indicator is referenced by an identifier (ID), this ID SHALL be used for exchanging contra-indicators between the IDP and the Identity Assurance Hub Operations Centre.

10.3. Contra-indicator scoring and mitigating actions

119. The User is to start the proofing process with a contra-indicator score of [redacted]. Each contra-indicator that is discovered attracts a score adjustment as described by the "found" value in the Contra-indicator Table.

120. If the IDP is able to resolve the contra-indicator by following the guidance as set out in the corresponding "Mitigating Actions" the risk score is further adjusted by the corresponding "pass" score. Where the IDP does not have the capability to perform the mitigating action then they cannot apply the 'pass' score. Many of the Mitigation Actions may in themselves raise further contra-indicators (where those Mitigating Actions fail), in such cases the new contra-indicator is simply treated as a contra-indicator in its own right.

10.4. Contra-indicators after registration

121. The IDP SHALL react to contra-indicators discovered after registration in the same manner as if they occurred during registration. The IDP SHALL evaluate whether they need to review the User's account to determine if they should continue to assert the Claimed Identity based on the information discovered.

122. In cases where the same check is performed at different times (e.g. those described by the Conditions for an Identity Assertion) then the following rules apply:
    - The result for the most recent check takes precedence; e.g. where a check returned [redacted] but later when the **same** check didn't return [redacted] then it is considered that there is now no [redacted] contra-indicator present from this check.
    - Results from different checks, regardless of the time between when they were done are considered as a whole, e.g. new contra-indictors discovered [redacted] after registration are added to all active contra-indicators discovered from the previous checks.

10.5. IPV Contra-indicators

ID	Contra-indicator	Details	Mitigating Actions	Found	Pass	FID
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

		[redacted]	[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

	[redacted]	[redacted]	[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]						
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]			

	[redacted]	[redacted]	[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

	[redacted]	[redacted]				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		

			[redacted]			
[redacted]						
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

			[redacted]			
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

		[redacted]				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		

		[redacted]				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]			

	[redacted]	[redacted]	[redacted]			

Table 16 Contra-Indicators

11. Suspicion of False Registration

11.1. Relationship between contra-indicators and potential false registration

123. Some contra-indicators may be discovered because the User is trying to register an identity that is not their own or are using falsified Identity Evidence. In cases where this is possibility a contra-indictor is also associated to a Failure Identifier (FID).

124. Simply because the IDP has discovered a contra-indicator that is associated with a FID does not in itself imply that there is an actual false registration only that there is a risk of it. In order to determine that there are reasonable grounds to suspect that a fraud may be taking place the FID SHALL need to be confirmed by following the mitigating actions associated with the contra-indicator.

125. Where the IDP does not have the capability to perform the mitigating action then they cannot apply the ‘pass’ score and by definition the FID cannot be ‘confirmed’.

126. If the IDP is able to resolve the contra-indicator then there is no suspicion of a false registration and the FID SHALL be ignored, however, if after taking the mitigating actions the IDP is still unable to resolve the contra-indicator then the FID SHALL be considered as being confirmed.

127. FIDs are mutually exclusive warnings and are prioritised as set out in the table below (Table 17 FID Prioritisation). Where an IDP has multiple confirmed FIDs then the one with the highest priority SHALL take precedence when returning a warning to the Identity Assurance Hub.

Priority	FID
1	[redacted]
2	[redacted]
3	[redacted]

Table 17 FID Prioritisation

12. Requirements for Assertion

12.1. Identity review (including revalidation)

128. The IDP SHALL have a review process in order to determine whether the Identity Evidence that has been validated under IPV Element B was reported lost, stolen or revoked soon after the original registration and/or whether the email address used has been confirmed as being under the control of the User.

129. The review required is dependent on the level of the identity and is described in the following table. When the timescale for the relevant review has been reached, the IDP must then perform the review before sending the assertion to the Identity Assurance Hub. Whether the identity review is performed at the time of an assertion or on the relevant date is a choice for the IDP.

Identity Level	Identity Review Requirements
1	▪ The IDP SHALL have confirmed that the email address is under the control of the User [redacted]
2	**Requirements for "Level 1" plus the following**: ▪ [redacted] the IDP SHALL ensure that all Identity Evidence that was confirmed as Valid during registration is still Valid, before the next assertion is made.
3	**Requirements for "Level 1" plus the following**: ▪ [redacted] the IDP SHALL ensure that all Identity Evidence that was confirmed as Valid during registration is still Valid, before the next assertion is made. ▪ The IDP SHALL have confirmed that the email address is under the control of the User [redacted]

Table 18 Identity Review

130. If Identity Evidence is found to no longer be valid at the review period then the IDP SHALL gather replacement Identity Evidence in line with GPG 45. Any new Identity Evidence SHALL be validated in accordance with GPG 45 and this document and SHALL be subject to the same review period, [redacted]

131. If Identity Evidence is determined to still be Valid after the final review period [redacted] then no [redacted]

12.1.1. Availability of external sources

132. Where the IDP uses a service provided by a 3rd party (e.g. the 'Document Checking Service') for Validation they may also allow an extension to the timeframes above in instances when the 3rd party service is unavailable to the IDP. This extension is limited [redacted] and only when it is due to the unavailability of the 3rd party service, this does not apply in instances where issues within the IDP prevent it accessing the 3rd party service.

12.2. Evaluating the identity

133. The IDP SHALL make a decision based on the information discovered from the IPV process on whether they should assert the User as the Claimed Identity. The IDP SHALL be confident that they can demonstrate the processes they performed and how they reached their decision in a court of law if required.

12.2.1. Promotion between Identity Levels

134. Where an IDP promotes a user between identity levels (e.g. from Level 1 to Level 2) then all the conditions required for the target Identity Level SHALL be met at the time of assertion. The IDP SHALL take into consideration all previous proofing done in the assessment for the higher Identity Level, including identity review, pause, resume and restarting of KBV, contra-indicators and conditions for Identity Assertion.

12.2.2. Demotion between Identity Levels

135. Where an IDP demotes a user between identity levels (e.g. from Level 2 to Level 1) then all the conditions required for the target Identity Level SHALL be met at the time of assertion.

136. Where the IDP decides to demote an account it MAY do this without performing the additional checks required for the existing higher Identity Level (i.e. the IDP does not attempt to maintain the Identity Level).

137. Where the IDP does perform the checks for the higher Identity Level the IDP SHALL take into consideration the outcome of those checks in deciding whether to assert the identity; a hard failure for a check at higher Identity Level that makes the account invalid (e.g. it is beyond the contra-indicator score threshold) this also prevents assertion at lower Identity Level even if that check was not required for the lower Identity Level [redacted].

12.3. Conditions for an Identity Assertion

138. The table below gives guidance on the conditions and circumstances required for asserting the Claimed Identity to the Identity Assurance

Hub. The conditions for Common apply in addition to the specific requirements at Identity Levels 1, 2 and 3.

Identity Level	Conditions for Assertion
Common	The IDP SHALL only assert the identity to the Identity Assurance Hub when all of the following conditions are met: ▪ The Identity Data shall contain the Claimed Identity. ▪ The IPV process is compliant with GPG 45 and this document. ▪ The IDP is confident that the User meets the requirements of the Identity Level requested as set out in GPG 45 and this document. ▪ The Credential (including process for issuance) is compliant with GPG 44 and this document. ▪ The User has successfully authenticated with the IDP using the relevant Credential. ▪ The IDP holds the relevant identity data in accordance with GPG 45 and this document. ▪ The IDP holds the relevant audit data as required by the Contract. ▪ The date of birth SHALL be verified. ▪ All applicable Identity Review conditions have been met.
1	**Requirements for “Common” plus the following**: ▪ The Identity Data SHALL contain at least one Personal Name marked as verified[redacted] ▪ The Identity Data SHALL contain at least one address marked as verified [redacted] ▪ The IDP SHALL have performed counter identity fraud checks (as defined by GPG 45 and this document)[redacted] ▪ [redacted]
2	**Requirements for “Common” plus the following**: ▪ The Identity Data SHALL contain at least one Personal Name marked as verified[redacted] ▪ The Identity Data SHALL contain at least one address marked as verified[redacted] ▪ The IDP has Activity History (as defined by GPG 45 and this document)[redacted] ▪ The IDP SHALL have performed counter identity fraud checks (as defined by GPG 45 and this document)[redacted] ▪ [redacted]
3	**Requirements for “Common” plus the following**: ▪ The Identity Data SHALL contain at least one address marked as verified[redacted] ▪ The IDP has Activity History (as defined by GPG 45 and this document) [redacted]

	▪ The IDP SHALL have performed counter identity fraud checks (as defined by GPG 45 and this document)[redacted] ▪ [redacted]

Table 19 Conditions for Assertion

12.4. Conditions for a warning

139. The table below gives guidance on the conditions and circumstances required for sending a warning to the Identity Assurance Hub and the appropriate code to be included.

Warning Code	Description	Conditions for code
IT01	Identity theft warning	This code SHALL be used when the contra-indicator score (after taking all mitigating actions) was at the threshold for the identity level (see Table 19 Conditions for Assertion) or lower plus one of the following conditions are also met: ▪ The IDP has reasonable grounds to suspect that the User is dishonestly making a false representation to an identity that is of another person and the IDP is prepared to report this to the Police. ▪ The User is not believed to the owner of the Claimed Identity because of the existence of a confirmed IT01 FID.
FI01	False identity warning	This code SHALL be used when the contra-indicator score (after taking all mitigating actions) was at the threshold for the identity level (see Table 19 Conditions for Assertion) or lower plus one of the following conditions are also met: ▪ The IDP has reasonable grounds to suspect that the User is dishonestly making a false representation to an identity that not of a real person and the IDP is prepared to report this to the Police. ▪ The Claimed Identity is not believed to be of a real person because of the existence of a confirmed FI01 FID.
DF01	Document fraud warning	This code SHALL be used when the contra-indicator score (after taking all mitigating actions) was at the threshold for the identity level (see Table 19 Conditions for Assertion) or lower plus one of the following conditions are also met: ▪ The IDP has reasonable grounds to suspect that the User may be possession of a false identity document (as defined by the Identity Documents Act 2010) and is prepared to report this to the Police.

		▪ The User may be possession of a false identity document because of the existence of a confirmed DF01 FID.

Table 20 Conditions for Fraud Warnings

12.4.1. Warning package

140. When the IDP sends a SAML response indicating that they have rejected a User because of a warning they SHALL make available the following information to the Identity Assurance Hub Operations Centre on request:
    - A fraud event number unique within the IDP
    - The Claimed Identity
    - All other information gathered/used during the IPV process
    - The PID
    - The FID code
    - All the contra-indicators discovered, the source of the contra-indicators and details of any remedial actions taken
    - Scores for the each of the IPV elements
    - Any other information the IDP used to determine that the User may not be genuine
    - [redacted]
    - Date, time and identifier of authentication request from the Identity Assurance Hub
    - Date, time and identifier of the SAML response from the IDP

12.5. Determining the Level of Assurance

141. The level of assurance reached by the user is a combination of the Level of the Identity (GPG 45) and the Level of Authentication (GPG 44). The following table demonstrates these combinations and the LoA achieved.

Level of Assurance				
		Level of Authentication		
		1	2	3
Level of Identity	None	N/A	0	0
	1	N/A	1	1
	2	N/A	2	2
	3	N/A	2	3
	4	N/A	2	4

Table 21 Level of Assurance

12.6. SAML Response to Identity Assurance Hub

142. If the IDP has met all the Conditions for an Identity Assertion then the IDP SHALL assert that the User has met the level of assurance to the Identity Assurance Hub with the Level of Assurance achieved, Claimed Identity, relevant history and other identity information required as defined by this document and the SAML profile.

143. If the IDP has determined that the User has failed to reach the level of assurance required but has not met the conditions for a warning then the IDP SHALL assert that the User has failed to reach the level of assurance to the Identity Assurance Hub.

144. If the IDP has determined that the User has failed to reach the level of assurance required and has met the conditions for a warning then the IDP SHALL return the Warning Code to the Identity Assurance Hub.