

WEB SERVICES INTERCHANGE AGREEMENT

Version 2.0

Date: 23rd November 2018

Contents

1. Introduction	33
2. Business Processes	44
2.1 Web Services Security	66
2.2 Web Service Time Out Details	77
2.3 Frequency	77
2.4 Web Service Availability Details	77
2.5 Data Retention	77
2.6 Volumes	77
2.7 Roles and Responsibilities	77
2.7.1 DBS	88
2.7.2 e-RB(s)/ROs	88
2.8 Service Level Agreements	88
3. Applicable Legislation	99
3.1 Data Protection Act 1998	99
3.2 Computer Misuse Act	99
3.3 Security Standards	99
3.4 Protective Marking of Data	99
4. Technical & Operational Security	1010
4.1 System Patching	1010
4.2 Malware / Anti-Virus	1010
4.3 Firewalls	1010
4.4 Content Checking/Blocking Policy.	1010
4.5 System Hardening and Secure Builds	1010
4.6 Protective Monitoring	1010
4.7 System Monitoring	1010
4.8 Physical and Personnel Security	1111
4.8.1 Physical Locations	1111
4.8.2 Systems and Users	1212
4.9 Cryptographic Material Handling	1212
5. Service and Interchange Management	1414
5.1 Monitoring and Reporting	1414
5.2 Problem Management and Escalation	1414
5.3 Interchange Agreement Review Procedure	1414
5.4 Accreditation Status of Interchange Agreement and Change Control Process	1414
5.5 Risk Assessment	1515
5.6 Disaster Recovery and Business Continuity	1515
5.7 Incident Handling	1515
5.8 Points of Contact	1515
Appendix A Glossary	1616
Appendix B Reference Documents	
Appendix C Operational Details	
C.4. Contact Dataila	4040

1. Introduction

This document details the Web Services Interface between the Disclosure and Barring Service (DBS), and the Registered Bodies(e-RBs) and Responsible Organisations (ROs) that are subscribed to use the service. The document defines:

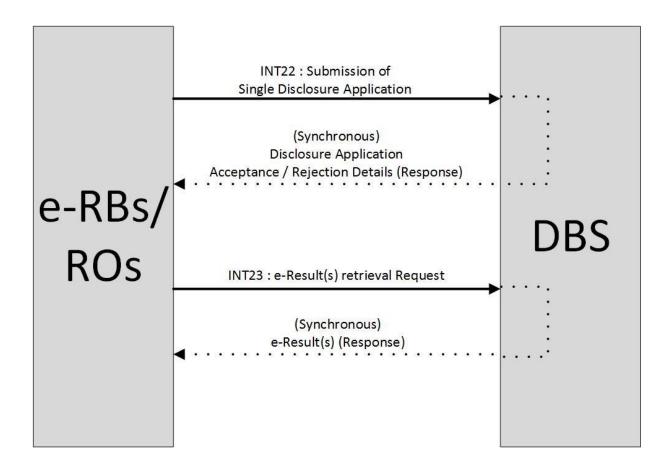
- Data exchange details
- · Business validation
- Security Governance Arrangements

The document has a target audience of:

- DBS Project Teams
- Implementers, developers and technical architects of the communicating endpoints
- Testers of the Web Services
- · Users of the Web Services

2. Business Processes

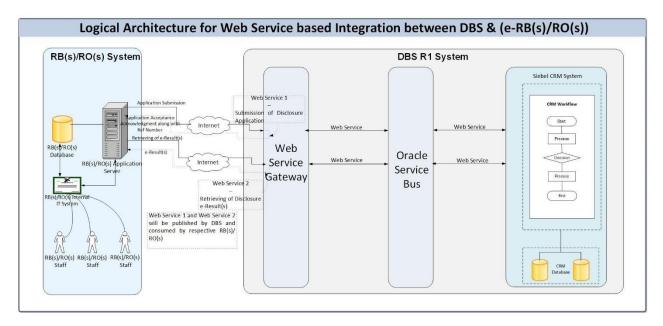
The Disclosure Web Services Interface allows e-RBs/ROs who are subscribed to use the Web Services Interface, to submit a Disclosure or Basic Application and to retrieve eResult(s) electronically via a web service(s) based interface mechanism.



Web Services Processes Overview

The Web Services Interface allows ROs and e-RBs, who are registered to use the Web Services Gateway, to submit Disclosure or Basic Applications electronically to the DBS and receive electronic notifications from the Web Services Gateway.

Note: Web Service provides a common base for connectivity and information exchange between business partners and the DBS. It allows systems based on different technology platforms to be integrated uniformly, and offers a variety of messaging services, such as transformation, reliability and routing to standardise this functionality across the system.



The diagram above illustrates the following:

- DBS hosts the following two web services (REST-based) over the internet in its environment, which are consumed by e-RB(s)/RO(s):
 - 1) Submitting a Disclosure or Basic Application
 - Retrieving e-Result(s) of processed applications

The above diagram depicts the following:

- Registered Bodies (e-RBs) / Responsible Organizations (ROs) consume DBS
 web service for sharing a single Disclosure or Basic Application. DBS provides a
 synchronous response to Registered Bodies (e-RBs) / Responsible
 Organizations (ROs) for accepting or rejecting an application for further
 processing.
- For an application that has been successfully validated by DBS a unique 'application reference number' is generated by the System.

- An application that has failed one or more business validation rules is 'rejected' and it is not considered for further processing. For each validation failure, a corresponding validation failure reason is generated.
- Registered Bodies e-RBs) / Responsible Organizations (ROs) consume a DBS web service for retrieving e-Result(s) for processed applications while sharing an application's unique identifier. DBS provides a synchronous response to Registered Bodies (e-RBs) / Responsible Organizations (ROs) while sharing eResult(s). In case of unavailability of e-Result(s), DBS also provides an appropriate response.

2.1 Web Services Security

- Standards based REST-based web services will be used
- End point authentication each end-point must be authenticated. For Internet web services client certificates will be used (see application authentication below)
- Application authentication each application end-point will be authenticated via a client certificate.
- SSL once authenticated all data traffic will be via SSL/TLS to and from the Web Services Gateway.
- End point and application authorisation each end point and application must be authorised for each web service it is consuming. For Internet facing web services authorisation by the Web Services Gateway will use certificates which will identify the organisation and each organisation will be authorised to access the web services that it has subscribed to.
- Ingress and egress data validation the web service input and output will be validated against the schema within the Web Services ICD.
- Ingress and egress content scanning all data being received via the web service will be content scanned for malicious content; all data being sent via the web service will be content scanned for malicious content
- Ingress and egress semantic scanning all data being received or sent via the web service will be scanned against any semantic rules, for example field formats and data value ranges
- Abnormal payload file size and record count upper and lower limit detection will be in place
- Auditing all web service interactions will be audited, this will be via web services auditing within the DBS solution
- Protective monitoring all web service interactions will be protectively monitored, this will be via web services protective monitoring within the DBS solution
- Credential aging all credentials used will be aged and must be changed before the issued certificate expires

- Zoning each web service terminates in the Web Services Gateway and will be cascaded into the core application by a process after all end-point checks and content inspection have been completed
- Failures authentication failures, authorisation failures or request processing failures will generate appropriate protective monitoring, auditing and system monitoring events as well as a defined error message to the web service calling end-point

2.2 Web Service Time Out Details

DBS web services will have a maximum time out limit of 30 seconds. In case of web service time out error, the e-RB(s)/ROs may re-try three times to share a web service request after 60 second intervals. In case of failure an incident will be raised with the DBS service management team. Message timeout details are configurable and will be reviewed during the design/testing phase.

2.3 Frequency

Each e-RB/RO can access DBS the Web Services Interface multiple times in each day. There is no specified schedule for e-RBs/ROs to access DBS web services.

2.4 Web Service Availability Details

The web services will be available (99% availability) throughout the day except from 12 am to 4 am (the scheduled maintenance window) within the constraints of the underlying hosting availability.

2.5 Data Retention

Disclosure or Basic Application data (available as part of application submission) will be retained as defined by the DBS retention policy (DBS 113 Retention Policy V1.0.doc).

2.6 Volumes

The following are the expected volumes for DBS Web Services:

1) Submitting Disclosure or Basic Application

Average Expected Web Service Transaction per day: 20,000

2) Retrieving e-Result(s) of processed applications (Disclosure outcome result)

Average Web Service Transactions per day: 20,000

2.7 Roles and Responsibilities

The roles and responsibilities described below have been defined for the Web Service interfaces.

2.7.1 DBS

DBS (Disclosure and Barring Service, the modernised solution) has the following responsibilities in ensuring that the interface functions correctly:

- Maintaining XML schemas (TCS will manage and maintain all XML schemas on behalf of DBS - all changes will be approved by DBS)
- Notifying the e-RB(s)/ROs of any change to existing XML schemas
- Authenticating the web service call
- Authorising the web service call
- Validating the data sent and received
- Acknowledging data received and responding with agreed success and error codes
- Monitoring for non-availability of the service or exceptions such as authentication or authorisation failures
- Notify e-RBs/ROs of planned maintenance windows and service downtime
- The issue and revocation of authentication credentials, i.e. electronic certificates.

2.7.2 e-RB(s)/ROs

The e-RB(s)/ROs have the following responsibilities in ensuring that the interface functions correctly:

- Notifying DBS if any changes are required to data attributes
- Access the DBS Web Service Interface while following DBS mandated authentication and authorisation mechanism
- Validating data shared by DBS
- Consuming DBS web services as per DBS guidelines
- Effective security governance
- Notification to DBS of security incidents
- Exercising due diligence in the protection of web service access certificates.
- Maintaining the security of authentication credentials such as usernames, passwords and certificates.
- Compliance with the Data Protection Act 1998 when processing DBS Applications.

2.8 Service Level Agreements

DBS and e-RB(s)/ROs must define appropriate business SLAs for this interface.

The DBS solution will provide a 99% SLA for availability of the service. Planned service outages will not count against this SLA.

The DBS solution will provide a 30 seconds SLA for confirmation of receipt of a submitted web service request.

3. Applicable Legislation

3.1 Data Protection Act 1998

The data exchanged between the client system and the Web Services Interface is covered by a registration / notification under the Data Protection Act. The information being exchanged is 'sensitive' personal information as defined under the Data Protection Act.

Information exchanged under this agreement must not be passed to third parties except where expressly permitted by DBS.

Web Services data must only be used for authorised purposes in connection with legitimate DBS business.

3.2 Computer Misuse Act

Users of the interconnected systems must comply with the Computer Misuse Act and must not attempt unauthorised access to the system.

3.3 Security Standards

The DBS system is required to conform to the DBS Accreditation Documentation Set, which includes various HMG security guidelines, and policies with which the system is required to conform. The DBS service operates within an ISO 27001:2013 Information Security Management System and has been through a HMG cyber security essentials assessment.

Software developed for use on the DBS system is required to be produced and maintained within an appropriate controlled development environment with documented standards. Code produced by clients for use with the DBS system to interface with the Web Services Gateway must conform to this.

3.4 Protective Marking of Data

The Web Services system processes and stores information that is protectively marked as OFFICIAL SENSITIVE. This equates to Personal Sensitive data under the Data Protection Act, as RO's and e-RB's do not work to government classifications.

The DBS system processes and stores information that is protectively marked as OFFICIAL SENSITIVE. This is in line with the Business Impact Assessment conducted by the DBS and consistent with the controls implemented as part of the IS1 technical risk assessments.

4. Technical & Operational Security

4.1 System Patching

Timely information about technical vulnerabilities of information systems being used by both parties shall be obtained, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk

4.2 Malware / Anti-Virus

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

4.3 Firewalls

Properly configured and tested boundary security devices, for example firewalls, must be installed on all systems with a connection to un-trusted networks, such as the Internet.

4.4 Content Checking/Blocking Policy.

Appropriate technical controls must be in place to monitor the content of traffic across the system boundary, especially boundaries with untrusted networks such as the Internet. This includes emails, Internet connections and business connections.

4.5 System Hardening and Secure Builds

A lockdown policy must be in place to restrict unnecessary services and ensure that no user or system component has more privilege (access and functionality) than required.

4.6 Protective Monitoring

To counter system and application attacks, a protective monitoring solution (that is a SIEM), will be implemented in the DBS live operational environment. Events and alerts will be produced and monitored in accordance with GPG13 guidelines.

Network and server log files and events will be passed to the protective monitoring solution for consolidation, archiving and reporting. The protective monitoring solution will automatically generate regular compliance reports which will be distributed to DBS Service Management for review.

Protective monitoring data shall be retained for a minimum of 12 months after which time it will be archived or erased and storage capacity shall be sized accordingly.

4.7 System Monitoring

System monitoring identifies if any of the infrastructure or application components that support the Business Services are not available or operating outside the defined SLAs. If any of the monitored components become unavailable or if there is performance degradation an alert will be generated. If any of the components are defined as service

affecting, these alerts also generate events, which can act as input to Service Desk Tool.

Business Service monitoring involves the following:

- Identification of the components of a business system
- Measuring the performance and availability of those components
- Identifying whether the components are performing within the Service Level Agreement
- Raising alerts/notifications on any deviation or potential deviation from the Service Level Agreement

The following list provides a summary of business services that are monitored and reported for Web Services;

- Process New Registration (e-RB / RO)
- Portal Login (e-RB / RO user)
- Web Services (Submit Disclosure or Basic Application, e-Result)

4.8 Physical and Personnel Security

The following physical and personnel security controls are applicable to this Interchange Agreement.

4.8.1 Physical Locations

Physical site security measures aim to either prevent a direct assault on premises or reduce the potential damage and injuries should an incident occur.

DBS and e-RB(s)/ROs must produce a physical and environmental policy which covers the security requirements of the site(s), system(s) and equipment to support the service delivery and the information processing requirements.

The policy will describe the physical controls that have been established for the following:

- Secure areas, including:
 - Physical security perimeter requirements
 - Physical entry controls
 - Securing offices, rooms, and facilities
 - Protection controls against external and environmental threats
 - o Requirements to be fulfilled for work within secure areas
 - Public access, delivery, and loading areas
- Equipment security, including:
 - Equipment siting and protection requirements
 - Security requirements for supporting utilities
 - Cabling security requirements
 - Security requirements for equipment maintenance

- Security of equipment off-premises
- Secure disposal or reuse of equipment
- Removal of property requirements

The policy will also specify assurance requirements to demonstrate compliance as follows:

- All records/evidence will be kept for a minimum of 12 months.
- Any deviation, failure or weakness must be recorded and reported to an Operational Security Manager.
- The DBS Security team may conduct scheduled or as-required audits to verify compliance with the policy.
- Suitable disciplinary action should be taken if anyone is found to have wilfully breached this policy.

e-RB(s)/ROs must ensure that a robust operational regime is in operation to ensure personnel security. All staff should be cleared according to their role and receive security awareness training as part of their induction process.

Users should sign all relevant policies to demonstrate they have understood their responsibilities in terms of personnel security and the use of DBS information assets and systems and this will form part of the operational security assurance regime.

Security Operating procedures (SyOps) will be in place for all staff detailing responsibilities for protecting the Confidentiality, Integrity and Availability of the DBS system, its resources and the data it contains.

4.8.2 Systems and Users

All users of the service are required to ensure the security of the servers and devices used to connect to the DBS solution. These must include:

- Patching of servers in line with industry best practice
- Use of an up to date anti-virus product suite
- Physical security of the service in line with industry best practice
- Policies and Procedures on the authentication of users to the system
- Incident reporting Policy and Procedure to notify the DBS help desk in the event of any incident that could affect the DBS system.

4.9 Cryptographic Material Handling

As part of using the DBS Web Services Interface DBS will send to the e-RB / RO electronic certificate(s) which contain key material which will authenticate access to the DBS Web Services Gateway and authorise access to the subscribed DBS web services. This certificate is sensitive and needs to be handled in a manner commensurate with its sensitivity.

The certificate shall be sent, via a secure channel, to a named individual within the e-RB / RO. The named individual shall be responsible for managing the certificate and maintaining the security of the certificate. This means that:

- 1. The certificate shall only be used in the context of the e-RB / RO to which it has been sent.
- 2. The e-RB / RO will ensure that the certificate is appropriately installed to facilitate web service use.
- 3. When not in use the certificate shall be stored securely under lock and key.
- 4. If the certificate is lost or compromised, the e-RB / RO shall inform the DBS help desk immediately.
- 5. If instructed to return the certificate this shall be done without question via an agreed secure channel.
- 6. If instructed to destroy the certificate, this shall be done under DBS instruction with an attestation certificate furnished.
- 7. As certificate expiry approaches, the e-RB / RO shall engage with DBS to ensure seamless certificate re-issue.

5. Service and Interchange Management

5.1 Monitoring and Reporting

The DBS Operational Security (OpSec) manager will ensure that the required logs and registers are maintained. The DBS OpSec manager or personnel authorised by him will perform audits on access to Web Services Interface data. These responsibilities are specified in the DBS OpSec manager Security Operating Procedures.

DBS staff should report problems with the interface to the Quality Management Manager who will liaise with the corresponding Web Services owner to resolve the problem.

5.2 Problem Management and Escalation

Suspected security breaches or problems should be reported to the DBS OpSec manager. The DBS OpSec manager will be responsible for managing and escalating problems as necessary with the appropriate system manager or DBS Security and for liaison with the security staff of the other system. This reporting is to be done via the DBS help desk.

Failure to comply with the security rules of this agreement or resolve any significant security problems raised in an acceptable time period may result in the Interchange Agreement and the connection being terminated.

5.3 Interchange Agreement Review Procedure

This Interchange Agreement will be reviewed annually by the DBS Data Controller and the Web Services Interface system data owner to ensure that planned benefits are being achieved and to identify any potential benefits which could accrue through further development of the facilities within the interfaces. It will also be reviewed annually by the DBS OpSec manager to ensure that security measures relevant to the interchange are still adequate in the light of any new or changed security threats.

If security measures are found to be no longer acceptable the Interchange Agreement may be terminated.

5.4 Accreditation Status of Interchange Agreement and Change Control Process

Any required changes to this agreement must be referred to, or raised by the DBS OpSec manager. The DBS OpSec manager will ensure that any proposed change is fully documented and justified prior to submitting to the systems security authorities for approval.

A proposed change may only be implemented after agreement by the DBS Security Committee and subsequent approval by the DBS Accreditation Authority and Web Services Interface system security authority. DBS representatives are members of the

DBS Security Committee and DBS Change Control Board (see DBS ADS Part 1, Security Roles, for membership of the DBS Security Committee and Change Control Board).

The DBS system change process is as documented in the TCS DBS Change Management Procedure.

5.5 Risk Assessment

A security risk assessment has been carried out by DBS. The results of this are documented in the DBS RMADS.

5.6 Disaster Recovery and Business Continuity

Business continuity for the interface is specified in the Web Services DBS Service Level Agreement.

Failure of the DBS workstations or network will be covered by the DBS system business continuity plan.

5.7 Incident Handling

The DBS Security Operating Procedures for DBS Core Staff and DBS OpSec manager specify the requirement to report security breaches to the DBS OpSec manager who will escalate incidents as necessary to the corresponding security authorities. Non-DBS users of the service are to report all incidents to the TCS Service Desk as soon as practicable upon identification of the incident.

5.8 Points of Contact

See Appendix C for nominated Point of Contact information.

Appendix A Glossary

The following terms, acronyms and abbreviations are used in this document:

Term	Definition	
CRM	Customer Relationship Management A solution to manage all interactions with the customer and support a superior customer experience across every channel	
CSV	Comma Separated Values File extension of a file containing data sets separated by commas, where each new line represents a new database row, and each database row has one or more fields separated by a comma. CSV files are commonly used for transferring data between databases in a simple text-based format	
DBS	Disclosure & Barring Service The UK Home Office department responsible for all disclosure and barring decisions in England and Wales Formed from a merging of the CRB and ISA	
DOB	Date of birth The day, month and year of birth	
HLD	High Level Design	
ICD	Interface Control Document	
LEA	Law Enforcement Agency	
LLD	Low Level Design	
LPF	Local Police Force The police organisation in a particular area	
MDM	Master Data Management A set of processes, governance, policies, standards and tools that consistently define and manage the master data of an organisation	
MF	Multi-system File	
Nominal data	A type of data in which there are limited categories but no order	

Term	Definition	
OSB	Oracle Service Bus	
	A scalable service-orientated architecture (SOA) integration platform that delivers an efficient, standards-based infrastructure for high-volume, mission critical SOA environments	
Web Services		
PNC	Police National Computer	
	A computer system used by law enforcement organisations in the UK containing information about convictions, cautions, reprimands and warnings	
PND	Police National Database	
POISE	Planned Office Information System Environment	
TCS	Tata Consultancy Services	
	The contractor selected for the DBS Programme	
UK	United Kingdom	
	Comprises England, Wales, Scotland and Northern Ireland, including the small adjacent islands, but not the Channel Islands or the Isle of Man	
	The full name is the United Kingdom of Great Britain and Northern Ireland	

Appendix B Reference Documents

The following documents are referred to in this document:

Ref	ID or Filename	Title and Description	Version	Date
1	TCS.04.996	Disclosure Web Services ICD v2.2	V2.2	27/06/2017
2	Requirements	Requirements Repository	V2.2	17/12/2013
3	TCS.04.147	External Interface Catalogue	V0.13	11/11/2014

Appendix C Operational Details

C.1 Contact Details

Details of technical and business contacts for TCS, DBS and the Web Services Gateway are given in the following table.

	DBS customer services: customerservices@dbs.gov.uk
	Telephone: 0300 0200 190
TCS Service Desk	Welsh: 0300 0200 191
	Minicom: 0300 0200 192
	International: +44 151 676 9390