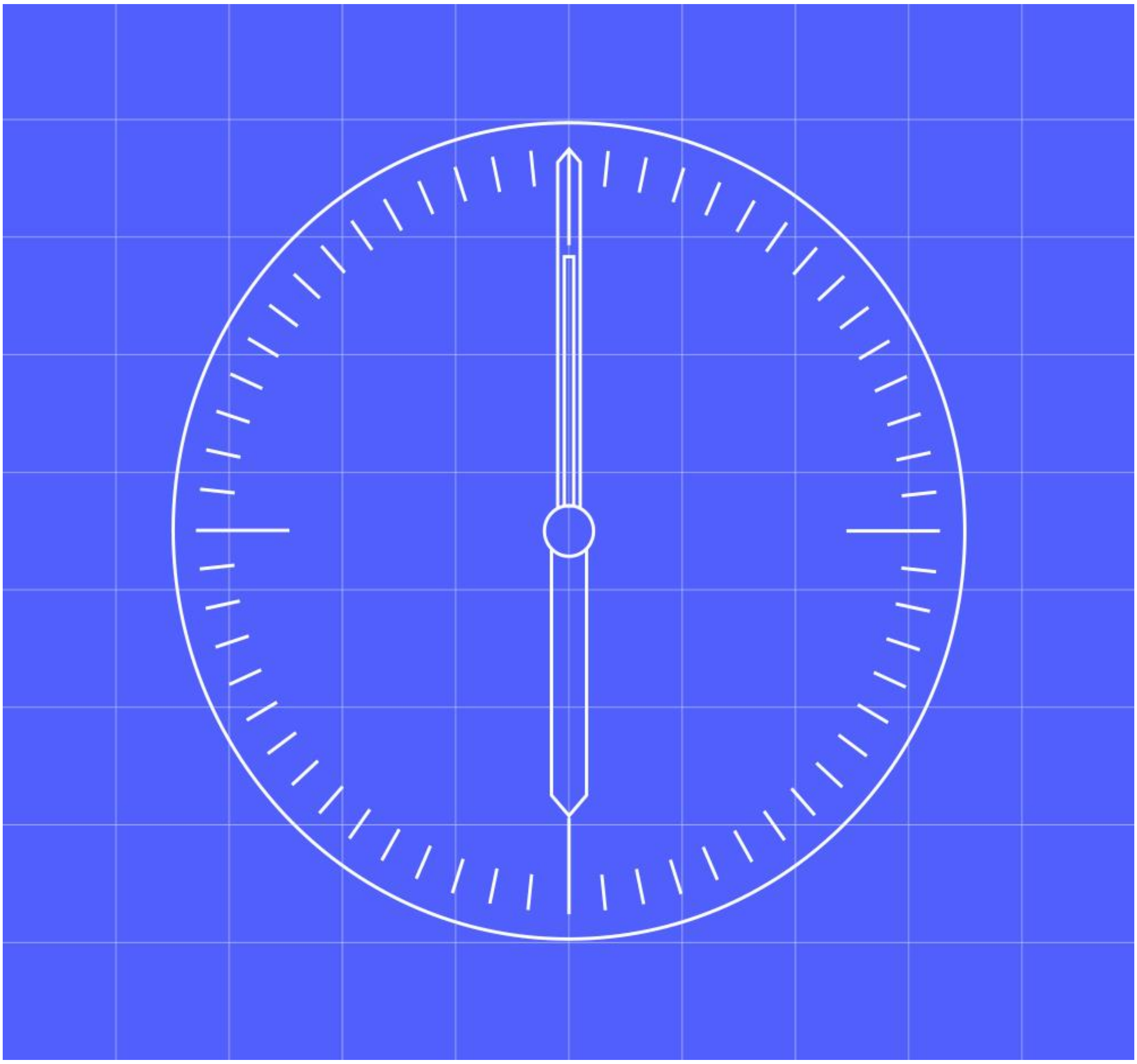
MHHS PROGRAMME
Industry-led, Elexon facilitated

Data Integration Platform PKI Policy



Document owner	Document number	Version	Status:	Date
MHHS DAG	**MHHS-DEL1210**	**Version 1.0**	**Approved**	**12th July 2023**

1 Table of Contents

1.1 Change Record

Date	Author	Version	Change Detail
24th April 2023	KG	0.1	Initial Draft
5th June 2023	KG	0.2	Updated broken link in section 5.6, updated section 5.9.9
19th June 2023	KG	0.3	Update – All sections post industry consultation
03rd July 2023	KG	0.4	Updated section 5.2.3 and changed all incorrect references from 7.1.1 to 8.7 (Certificate Profile)
12th July 2023	KG	1.0	DAG Approval

1.2 Reviewers

Reviewer	Role

1.3 References

Document/Link	Publisher	Published	Additional Information
MHHS-DEL1197 - Interface Code of Connection	MHHS	V0.6	May 2023
Certificate practice statement	GlobalSign		https://www.globalsign.com/en/repository/GlobalSign_CPS_v6.5.pdf

1.4 Terminology

Term	Description
CoCo	MHHS DIP094 - Interface Code of Connection
CRL	Certificate Revocation List
DCA	DIP Certificate Authority
DCP	DIP Connection Providers – Third Parties, Software Providers, Academia etc.
DIP-PKI	Public Key Infrastructure Policy
DIP-PKI CM	Certificate Manufacturer
DIP-PKI CP	This Policy (See RFC3647 for further details)
DIP-PKI CPS	Certificate Practice Statement (See RFC3647 for further details)
DIP-PKI CRL	Certificate Revocation List
IETF	Internet Engineering Task Force - https://www.ietf.org/
RFC	Request For Comments - https://www.ietf.org/standards/rfcs/
PKI	Public Key Infrastructure

2 INTRODUCTION

2.1 OVERVIEW

This document forms part of the DIP Manager Role and in conjunction with the Code of Connection (CoCo) sets out the requirements for the DIP Public Key Infrastructure environment. The DIP Manager in its role as the Policy Authority (See 2.3.6.1 below) has published this DIP-PKI Certificate Policy document which is a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements, i.e. the DIP Messaging Service. The DIP-PKI Certificate Policy document is structured in accordance to the guidelines in IETF RFC 3647, with appropriate modifications, deletions and references to other documentation as appropriate. This Certificate Policy defines a Public Key Infrastructure and in conjunction with the PKI Disclosure Statement, specifies:

- Who can participate in the Public Key Infrastructure defined by this Certificate Policy
- The primary rights, obligations and liabilities of the parties governed by this Certificate Policy
- The purposes for which Certificates Issued under this Certificate Policy may be used
- Minimum requirements to be observed in the issuance, management, usage and reliance upon Certificates

2.2 DOCUMENT NAME AND IDENTIFICATION

This document is titled The DIP-PKI (Public Key Infrastructure) Policy. In short and where applicable in this document the DIP-PKI, The Policy.

2.3 PKI Participants (DIP SERVICE USERS)

The DIP Manager has an obligation to operate a PKI environment in accordance with this Policy it defines and publishes. There are sets of functions that are logically and conveniently grouped and delegated.

:

For purposes of this policy document the DIP Manager is referred to as the Issuing Authority IA

- Certificate Authority (DIP Manager)
- Policy Authority (DIP Manager)
- Trust Service Providers
- Issuing Authority (DIP Manager) owns the PKI
- Certificate Manufacturer CM - (GlobalSign)
- Registration Authority (DIP Manager)
- Repository (DIP Manager/ GlobalSign)
- End Entities
    - DIP Service Users are listed in the Code of Connection (CoCo) section 5.6.
- Relying Parties to this service, including the Relying Party Agreement, are detailed in the CoCo section 5.7.

2.3.1 CERTIFICATION AUTHORITIES

Certification Authorities are the entities that Issue Certificates i.e. trust service providers and the Certification Authority is synonymous with Issuing Authority.

2.3.1.1 *ISSUING AUTHORITY*

By definition, an Issuing Authority is the entity listed in the Issuer field of a Certificate. The Issuing

Authority “owns” the service and has the ultimate responsibility for deciding who may be issued with a

Certificate carrying its name as the Issuer. The Data Communications Company (DIP Manager) is the Issuing Authority.

2.3.1.2 *CERTIFICATE MANUFACTURER*

GlobalSign. Is the Certificate Manufacturer and provides the infrastructure and operational services for the DIP Manager in relation to the manufacture of Certificates.

The Certificate Manufacturer has no authority to make decisions on the Issuance of Certificates, or other aspects of certificate management outside of the certificate manufacturing process. The Certificate Manufacturer operates under the direction of the Issuing Authority.

The Certificate Manufacturer must demonstrate compliance with this Policy. Compliance is documented and controlled via the DIP Certification Practice Statement (CPS). Where this is complemented by additional supporting documentation it is referred to generically in this Certificate Policy with the term Certificate Manufacturer Procedures.

2.3.2 REGISTRATION AUTHORITY

The DIP Manager is the Registration Authority.

The Registration Authority is responsible for ensuring the eligibility of applicants to be issued with Certificates together with the accuracy and integrity of required information presented by applicants. The Registration Authority's role is to process and approve requests from applicants for the Issue of Certificates or for their Revocation, Suspension as detailed elsewhere in this Policy.

For the purposes of this Certificate Policy and operating model, there will be a single Registration Authority.

For purposes of this policy document, where activities are apportioned to the Registration Authority, that will be replaced with the Issuing Authority or IA as applicable.

2.3.3 DIP SERVICE USERS

A DIP Service User is an End-Entity (such as a person or organization) that has applied for and received a Certificate. The DIP Service User bears responsibility for the use and security of the Private Key associated with the Certificate. See the CoCo section 5.6 for further details.

2.3.4 SUBJECTS

DIP Service Users may use a 3rd Party, such as a DIP Connection Provider, to represent them as an authorized representative acting on behalf of the DIP Service User (Market Participant). A DIP Service Users using a subject who is an employee of a DIP Connection Provider is ultimately responsible for ensuring the subject complies with the DIP-PKI Policy (this document). In all cases, the DIP Service User is responsible for compliance with the DIP-PKI Certificate Policy and all other obligations applicable to it and the Subject.

See section 5.6 of the CoCo for further details.

2.3.5 RELYING PARTIES

Relying Parties are those entities that are using a Certificate to authenticate another Certificate Subscriber named in the Certificate. In the context of the DIP, every Certificate Subscriber is also a Relying Party at some point in the process of exchanging messages with the DIP and DIP Service Users.

Relying Parties are subject to the requirements of the Relying Party Obligations as set out in the CoCo section 5.7

2.3.6 OTHER DIP SERVICE USERS

2.3.6.1 *POLICY AUTHORITY*

The Policy Authority has responsibility for control over the Issuance, management and usage of Certificates Issued under this Policy.

2.3.6.2 *REPOSITORY*

The Repository is managed by the DIP Manager and holds data in support of PKI operations. This includes policy and related documentation, Certificates and Certificate Status information.

The Repository provides a community-wide accessible mechanism by which primarily DIP Service Users and Relying Parties can obtain and validate information on Certificates Issued under this Certificate Policy.

The Issuing Authority is responsible for providing the DIP-PKI Repository in accordance with this Policy.

See section 3 of the CoCo for further details.

2.4 CERTIFICATE USAGE

Certificate usage is defined by the Certificate Profile. Certificate Profiles are approved and issued by the DIP Manager.

A) The DIP Manager shall ensure that DIP-PKI Certificates are issued only:

1. To Eligible DIP Service Users and
2. For the purposes of:
    a. The creation, sending, receiving and processing of communication within the DIP environments in accordance with or pursuant to the DIP Manager or the Service Definition which will further include
        I. Symmetric key generation (Digital Signature, Key Agreement);
        II. TLS Communication (Digital Signature, Key Agreement, TLS Web Client Authentication, TLS Web Server Authentication); and
        III. Authentication and Non-Repudiation (Digital Signature, Non-Repudiation, Key
        IV. Encipherment, Data Encipherment, Key Agreement, TLS WebClient Authentication. TLS Web Server Authentication)

2.4.1.1 *APPROPRIATE CERTIFICATE USES*

See part 2.3 above of this DIP-PKI Policy

2.4.1.2 *PROHIBITED CERTIFICATE USES*

All other application use and any other usage categories, other than what has been detailed in the DIP Service User Agreement and the Relying Parties Agreement, for Certificates Issued under this Policy is prohibited.

2.5 STATEMENTS ADMINISTRATION

2.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The DIP Manager, under its function as the Policy Authority, is responsible for approving rights, obligations and all other terms and conditions contained in this Certificate Policy.

2.5.2 CONTACT PERSON

Questions in relation to the content of this Policy should be made to:

DIP Manager

350 Euston Rd,

London

NW1 3AW

2.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE STATEMENTS

The DIP Manager determines the suitability of any DIP-PKI Certification Practice Statement (CPS) operating under this policy.

2.5.4 CPS APPROVAL PROCEDURES

The DIP-PKI CPS is subject to periodic internal reviews by the DIP Manager.

The DIP Manager shall keep the DIP-PKI CPS under review and shall in particular carry out a review of the DIP-PKI CPS including a review by an independent party - whenever and to the extent to which it may be required to do so in line with its duties as set out by the DIP Manager in providing the PKI service.

Following any review of the DIP-PKI CPS the DIP Manager may propose amendments to it.

2.6 DEFINITIONS AND ACRONYMS

Definitions of the terms used in this Policy are detailed in the glossary at the end of this document.

3 PUBLICATION AND REPOSITORY RESPONSIBILITIES

3.1 REPOSITORIES

The DCA and the DIP-PKI Certificate Manufacturer each have their own repositories.

The DIP-PKI Repository associated with the DIP-PKI Operator Root CA Certificates (DIP-PKI Certificate Manufacturer) stores the following information:

- All copies of issued DIP-PKI Operator Root CA Certificates
- Certificate status and validity meta-data for each DCA Certificates

The DIP-PKI Repository associated with End Entity Certificates shall store the following information:

- All copies of DIP-PKI End Entity Certificates issued by the DIP-PKI Operator CA
- Certificate status and validity meta-data for each DIP-PKI End Entity Certificate issued
- The latest version of the DIP-PKI CRL (Certificate Revocation List) all copies of issued DCA Certificates See CoCo section 6 for details.

3.2 PUBLICATION OF CERTIFICATION INFORMATION

See section 2.1 of this Policy

3.3 TIME OR FREQUENCY OF PUBLICATION

The DCA Shall ensure that:

- Each DIP-PKI End Entity Certificate is promptly accepted by a DIP Service User when issued;
- Each DIP-PKI Certificate is lodged in the applicable Repository promptly on being issued;
- The DIP-PKI CRL is lodged in the DIP-PKI Repository within such time as specified in Part 5.7 of this Policy.

3.4 ACCESS CONTROLS ON REPOSITORIES

All DIP-PKI Repositories are subject to access controls using usernames and passwords. Only authorized DIP-PKI Systems Personnel have access to DIP-PKI Repositories.

.

4 IDENTIFICATION AND AUTHENTICATION

4.1 NAMING

4.1.1 TYPES OF NAMES

The DCA shall ensure that the name of the entity that is the Subject of each Certificate is in accordance with the relevant Certificate Profile.

See section 8.7 of the CoCo for details.

4.1.2 NEED FOR NAMES TO BE MEANINGFUL

The DCA shall ensure that the name of the Subject of each certificate is meaningful and consistent with the relevant Certificate Profile.

See section 8.7 of the CoCo for details.

4.1.3 ANONYMITY OR PSEUDONYMITY OF DIP SERVICE USERS

The anonymity or pseudonymity of DIP Service Users is not supported under this Policy.

4.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

The interpretation of common fields is given in the CoCo section 8.7for details.

4.1.5 UNIQUENESS OF NAMES

Provision in relation to the uniqueness of names is made in the CoCo section 8.7 for details.

4.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

No eligible DIP Service User may make a Certificate Signing Request which contains:

- Any information that constitutes a trademark unless it is the holder of the Intellectual Property Rights in relation to that trademark or

Any confidential information which would be contained in a Certificate issued in response to that Certificate Signing Request.

4.2 INITIAL IDENTITY VALIDATION

4.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

Provision is made in section 6.2 of the CoCo in relation to:

- The procedure to be followed by an Eligible DIP Service User in order to prove its possession of the Private Key which is associated with the Public Key to be contained in any certificate that is the subject of a Certificate Signing Request and
- The procedure established for this purpose is in accordance with the procedure in PKCS#10or an equivalent cryptographic mechanism.

4.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

The DIP Manager will authenticate the organisation in accordance with the on-boarding process. See section 5.4 of the CoCo for further details.

4.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

Provisions are made in section 5.4.1 of the CoCo in relation to the authentication of persons eligible to request certificates

4.2.4 VALIDATION OF AUTHORITY

See section 4.2.2 of this Policy

4.2.5 CRITERIA FOR INTEROPERATION

Not applicable to this Policy.

4.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

4.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

This Policy does not support Certificate Re-Key and therefore will not provide a Re-Key Service.

4.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Not applicable to this Policy.

4.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Provision is made in section 6.1.3 of the CoCo in relation to procedures designed to ensure the authentication of DIP Service Users who submit a Certificate Revocation Request to ensure they are authorized to submit that request.

5 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

5.1 CERTIFICATE APPLICATION

5.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

Provisions have been made in the CoCo section 6.1.2 in relation to the circumstances in which an Eligible DIP Service User may submit a Certificate Signing Request, the procedures to be followed and the means by which it may do so.

5.1.2 ENROLMENT PROCESS AND RESPONSIBILITIES

The DIP Manager has made provisions for the establishment of a registration process in respect of organizations requiring Certificates. See CoCo section 5.4

5.1.2.1 *REGISTRATION AUTHORITIES AND THEIR REPRESENTATIVES*

For the purposes of this DIP-PKI operating model, there will be only 1 (one) Registration Authority who will be the DIP Manager.

5.2 CERTIFICATE APPLICATION PROCESSING

5.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

Provision is made in the CoCo section 6 in relation to the Authentication by the DCA of Eligible DIP Service Users who submit a Certificate Signing Request.

5.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

Where any Certificate Signing Request fails to satisfy the requirements set out in the CoCo section 6 the DCA:

- Shall reject it and refuse to issue the Certificate which was the subject of the Certificate Signing Request and
- Shall give notice to the Party which made the Certificate Signing Request of the reasons for its rejection.

Where any Certificate Signing Request satisfies the requirements set out in the CoCo section 6 the DCA shall issue the Certificate which was the subject of the Certificate signing Request.

5.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

All Certificate Signing Requests will be processed 7 seconds upon receipt of request.

Upon receipt and successful validation of a Certificate Signing Request, the DCA will promptly issue a Certificate in response.

5.3 CERTIFICATE ISSUANCE

5.3.1 DCA ACTIONS DURING CERTIFICATE ISSUANCE

The DCA will issue a Certificate only:

- In accordance with the provision in this Policy and requirements of the CoCo sections 3, 5 and 6
- In response to a Certificate Signing Request made by an Eligible DIP Service User The DCA shall ensure that:
  - Each DCA Certificate issued by it contains information that it has verified to be correct and complete and
  - Each DIP-PKI End Entity Certificate issued by it contains information consistent with the information in the Certificate Signing Certificate.

A DIP-PKI Certificate may only be:

- Issued by the DCA and
- For that purpose, signed using a DCA Private Key.

The DCA shall not issue:

- A DCA Certificate using an Operator Root CA Private Key after the expiry of the Validity Period of an

Operator Root CA Certificate containing the Public Key associated with that Private Key;

- A DIP-PKI End Entity Certificate using a DCA Private Key after the expiry of the Validity Period of an DCA Certificate containing the Public Key associated with that Private Key; or
- Any Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Certificate that was previously issued by it.

5.3.2 NOTIFICATION TO DIP SERVICE USER BY THE DCA OF ISSUANCE OF CERTIFICATE

Provision is made in the CoCo section 6.1.1 for the DCA to notify an Eligible DIP Service User where that Eligible DIP Service User is issued with a Certificate which was the subject of a Certificate Signing Request made by it.

5.4 CERTIFICATE ACCEPTANCE

5.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

A Certificate which has been issued by the DCA shall be treated as valid for any purpose of this Certificate Policy until such time as it is revoked.

The DCA shall maintain a record of all Certificates which have been issued by it and accepted by a DIP Service User.

5.5 KEY PAIR AND CERTIFICATE USAGE

5.5.1 DIP SERVICE USER PRIVATE KEY AND CERTIFICATE USAGE

Provision for restrictions on the use by DIP Service Users (Users) of Private Keys in respect of Certificates is made in this Policy.

5.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Relying Party obligations are set out in the CoCo section 5.7

5.6 CERTIFICATE RENEWAL

Currently, every certificate issued by the DCA for the DIP will have a validity period of 398 days. Prior to expiry a DIP User with a PKI role if SRO, ARO or TC should generate a new CSR and get it signed via the DIP User Portal, the process for this is the same as 5.3 Table of ContentsCERTIFICATE ISSUANCE.

As all requests for signing come through the DIP User portal, the portal will notify the DIP Users (See CoCo section 5.4.3 Roles privilege Table) hat a certificate is about to expire and therefore that they should generate a new CSR and get it signed via the DIP portal.

Notifications of certificate expiry will be sent to the DIP Service User Administrator at the following intervals;

- 90 days prior to the certificate expiring
- 60 days prior to the certificate expiring
- 30 days prior to the certificate expiring
- 1 day prior to the certificate expiring.

The new certificate will start from the date the Certificate Signing Request has completed and not the date the current certificate expires.

- Current certificates will remain valid until the expiry date expires and will continue to run alongside the new certificate allowing a grace period for seamless transfer.

5.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

Certificate renewal is defined as the production of a new Certificate that has the same details as a previously issued Certificate and the same Public Key.

The DCA may renew Certificates which have either been previously renewed or previously rekeyed (subject to the points above). The original Certificate may be revoked after renewal is complete; however, the original Certificate must not be further renewed, re-keyed or modified.

5.6.2 WHO MAY REQUEST RENEWAL

SRO, ARO, TC

See CoCo section 6.1.4

5.7 CERTIFICATE REVOCATION AND SUSPENSION

A certificate may need to be revoked for several reasons.

An approved SRO/ARO/TC (Technical contact) can revoke certificates using the DIP User Portal following the process below:

- From within the portal, the service user navigates to the certificates page, the DIP Service User will be shown their current certificates.
- Under the certificate actions option, they can choose Revoke.
    - To revoke a certificate a reason for revocation must be entered from selected from a list of possible reasons:
- On submission of the reason, the DIP portal will use the organsiations API credentials and mTLS certificate, to call the DCA and request the certificate is revoked.
- The DIP portal will inform the DIP Service User Administrator that the certificate is successfully revoked.

Once revoked the certificate will no longer be valid when calling the DIP as either the mTLS or message signing certificate. During the process of mTLS or message signing the Online Certificate Status Protocol (OCSP) is called. The OCSP is a property of the certificate and is an endpoint that specifies the certificate status (valid/revoked).

5.7.1 CIRCUMSTANCES FOR REVOCATION

A DIP Service User shall ensure that it submits a Certificate Revocation Request through the DIP User Portal in accordance with this Certificate Policy and:

- Immediately upon becoming aware that the Certificate has been Compromised, or is suspected of having been Compromised; or
- Immediately upon ceasing to be an Eligible DIP Service User in respect of that Certificate

A Certificate must be Revoked:

- When any of the information in the Certificate is known or suspected to be inaccurate.
- Upon suspected or known compromise of the Private Key associated with the Certificate.
- Upon suspected or known compromise of the media holding the Private Key associated with the

- Certificate.

The DCA may revoke a Certificate when if a DIP User Organisation fails to comply with any obligations set out in this Certificate Policy.

5.7.2 WHO CAN REQUEST REVOCATION

Any SRO, ARO or TC may submit a Certificate Revocation Request in relation to a Certificate for which it is the Authorised DIP Service User and shall on doing so by specifying its reason for submitting the Certificate Revocation Request.

5.7.3 PROCEDURE FOR REVOCATION REQUEST

Provision is made in the CoCo section 6.1.3 in relation to the procedure for submitting and processing a Certificate Revocation Request.

5.7.4 REVOCATION REQUEST GRACE PERIOD

None. If the Revocation request is approved, it must be reflected in the next scheduled publication of Certificate Status Information.

5.7.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

The DCA shall ensure that it processes all Certificate Revocation Requests within 24 hours depending on the reason for the request.

The mechanisms, if any, that a Relying Party may use in order to check the Certificate Status Information of the Certificate upon which they wish to rely, must be via Certificate Revocation Lists or equivalent online protocol that permits authenticity and integrity of the Status Information to be verified

5.7.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Provision is made in the CoCo section 6.1.3 in relation to the procedure for submitting and processing a Certificate Revocation Request.

5.7.7 CRL ISSUANCE FREQUENCY

The DCA shall ensure that an up to date version of the DIP-PKI CRL is lodged in the relevant DIP-PKI Repository at least once in every period of 48 hours.

Each version of the DIP-PKI CRL shall be valid until 48 hours from the time at which it is lodged in the DIP-PKI Repository.

Further provision in relation to the reliance that may be placed on the DIP-PKI CRL (and on versions of it) is set by the DIP Manager.

The DCA shall ensure that each up to date version of the DIP-PKI CRL:

- Continues to include each relevant revoked Certificate until such time as the Validity Period of that certificate has expired; and
- Does not include any revoked Certificate after the Validity Period of that Certificate has expired.

The DCA shall ensure that the DIP-PKI CRL contains a non-critical entry extension which identifies the reason for the revocation of each Certificate listed on it in accordance with RFC 5280.

The DCA shall retain a copy of the information contained in all versions of the DIP-PKI CRL together with the dates and times between which each such version was valid. This information shall be made available as soon as is reasonably practicable, on receipt of a request, to the DIP Manager, Ofgem any DIP Service User (user) or any Relying Party.

5.7.8 ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY

The availability of on-line Certificate Status checking shall be published by the DCA every 48 hours.

5.7.9 ON-LINE REVOCATION CHECKING REQUIREMENTS

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates:

- OCSP responses MUST have a validity interval greater than or equal to eight hours.
- OCSP responses MUST have a validity interval less than or equal to ten days.
- For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
- For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates:

- The DCA shall update information provided via an OCSP Responder (i) at least every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate. OCSP Responders that receive a request for status of a Certificate that has not been issued, shall not respond with a "good" status for such Certificates. OCSP Responders for CAs which are not Technically Constrained, in line with section 8.1.5, shall not respond with a "good" status for such Certificates.

5.7.10 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

Not applicable to this Policy

5.7.11 SPECIAL REQUIREMENTS OF KEY COMPROMISE

Where any Private Key is Compromised, then the DCA shall :

- Immediately notify the DIP Manager;
- Provide the DIP Manager with all of the information known to it in relation to the nature and circumstances in the event of Compromise or suspected Compromise;
- and where the Compromise or suspected Compromise relates to any Private Key;
    - Ensure that the Private Key is no longer used;
    - Promptly notify each of the Authorised DIP Service Users for any Certificates Issued using that Private Key.

5.7.12 CIRCUMSTANCES FOR SUSPENSION

This Policy does not support Suspension of DIP Service User Certificates.

5.8 CERTIFICATE STATUS SERVICES

5.8.1 OPERATIONAL CHARACTERISTICS

The types of Certificate Status checking services made available to the DIP Service User by the Repository will be as certificates are issued or within 48 hours.

5.8.2 SERVICE AVAILABILITY

TBC.

5.8.3 OPTIONAL FEATURES

Not applicable in this Policy

5.9 END OF SUBSCRIPTION

Each DIP-PKI certificate has a lifecycle of 398 days in each environment. At the end of the subscription the relevant DIP Service User Certificates may either be Revoked or permitted to expire. Provision have been made for notification by the DCA to the DIP Service User.

5.10 KEY ESCROW AND RECOVERY

5.10.1 KEY ESCROW AND RECOVERY STATEMENTS AND PRACTICES

This Policy does not cover Key Escrow services

The DCA shall not provide any Key Escrow services

The DIP-PKI Recovery practices are documented in the DIP-PKI CPS

6 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The facilities, management and operational controls for the manufacture of certificates are managed through a Trusted Service Provide in GlobalSign Europe, identified herein as DIP-PKI CM.

The DIP-PKI CM shall ensure that the DIP-PKI CPS incorporates detailed provision in relation to the facility, management, and operational controls to be established and operated for the purposes of the exercise of its functions as the DIP-PKI CM

6.1 PHYSICAL CONTROLS

6.1.1 SITE LOCATION AND CONSTRUCTION

The Issuing Authority shall ensure where Certificate manufacture or time-stamping operations are carried out must:

- Satisfy at least the requirements specified by either ISO 27001, ETSI TS 319 401 for CAs for production and control of Certificates.

- Be manually or electronically monitored for unauthorised intrusion at all times.
- Apply controls such that unescorted access to CAs or time-stamping servers is limited to authorised personnel.
    - Ensure unauthorised personnel are properly escorted and supervised.
    - Ensure a site access log is maintained and inspected periodically.
- Ensure all removable media and paper containing sensitive plain text information is stored in secure containers.

6.1.2 PHYSICAL ACCESS

See section 6.1.1

6.1.3 POWER AND AIR CONDITIONING

The DIP-PKI Certificate Manufacturer (CM) shall ensure adequate provisions in relation to power and air conditioning at all physical locations in which the DIP-PKI Systems are manufactured.

6.1.4 WATER EXPOSURES

The DIP-PKI CM shall ensure that the DIP-PKI CPS incorporates provisions in relation to water exposure at all physical locations in which the DIP-PKI Systems are manufactured.

6.1.5 FIRE PREVENTION AND PROTECTION

The DIP-PKI CM shall ensure that the DIP-PKI CPS incorporates provisions in relation to fire prevention and protection at all physical locations in which the DIP-PKI Systems are manufactured.

6.1.6 MEDIA STORAGE

The DIP-PKI CM shall ensure that the DIP-PKI CPS incorporates provisions designed to ensure that appropriate controls are placed on all media used for the storage of Data held by it for the purposes of carrying out its functions.

6.1.7 WASTE DISPOSAL

The DIP-PKI CM shall ensure that the DIP-PKI CPS incorporates provisions designed to ensure all media used to store Data held by it for the purposes of carrying out its functions are disposed of only using secure methods.

6.1.8 OFF-SITE BACKUP

The DIP-PKI CM shall ensure off site backup arrangements must be in place as required by the business continuity arrangements outlined in section 6.7

Where data and facilities are removed from primary locations or in support of business continuity activities, controls must be applied which are at least comparable with those of the primary location.

6.2 PROCEDURAL CONTROLS

6.2.1 TRUSTED ROLES

The DIP-PKI CM shall provide for the separation of distinct PKI personnel roles by named personnel, distinguishing between day-to-day operation of the CA system and the management and audit of those operations. To the greatest extent possible, differing levels of physical and systems access control based on roles and responsibilities shall be employed to reflect the requirements of those roles and responsibilities. Controls must be detailed in the Certification Practice Statement and/or supporting documentation.

The Issuing Authority, in performing its role as the registration authority shall ensure that all

Registration Authority personnel are adequately trained and understand their responsibility for the identification and authentication of prospective DIP Service Users and related Certificate management tasks. Registration Authorities shall document arrangements for trusted roles in the Registration Policy and Procedures and/or supporting documentation.

The Issuing Authority may permit all roles and duties for Registration Authority functions to be performed by one individual.

6.2.2 NUMBER OF PERSONS REQUIRED PER TASK

The DIP-PKI CM shall ensure multi-person controls are established for the performance of critical functions associated with the build and management of CA systems, including the software controlling Certificate manufacturing operations.

All other duties associated with Certificate Manufacture may be performed by an individual operating alone, provided verification processes employed must provide for oversight of all activities performed by trusted role holders.

6.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

The DIP-PKI CM shall ensure personnel in trusted roles are formally appointed and approved to hold the position. They shall have their identity and authorisation verified before they are:

- Included in the access list for the site of the DIP Service User providing Trust Services.
- Included in the access list for physical access to the Trust Service provider systems.
- Given a credential for the performance of their Trust Service provider role.
- Given an access on Trust Service provider systems.

Credentials issued to personnel in trusted roles must be:

- Managed so that their use can be detected and monitored
- Managed so that their use is restricted to actions authorised for that role through applicable technical and procedural controls.
- Maintained under a prescribed and documented security policy
    - Maintained under a prescribed and documented security policy.
- Maintained under a prescribed and documented security policy.

6.2.4 ROLES REQUIRING SEPARATION OF DUTIES

The DIP-PKI CM in its assignment of duties among personnel shall maintain appropriate separation of duties so as not to compromise the security arrangements for the Certificate Manufacturing and other critical processes. The Certificate Manufacturer shall provide and maintain records of role allocation.

6.3 PERSONNEL CONTROLS

6.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

The DIP-PKI SP shall ensure that all personnel performing duties with respect to its operation must:

- Be appointed in writing.
- Be bound by contract or statute to the terms and conditions of the position they are to fill.
- Have received training with respect to the duties they are to perform.
- Be bound by statute or contract not to disclose sensitive security-relevant information or DIP Service User information and maintain required protection of personal information.
- Not be assigned duties that may cause a conflict of interest with their service provision duties.
- Not have been, as far as known, previously relieved of a past assignment for reasons of negligence or non-performance of duties.

6.3.2 TRAINING REQUIREMENTS

See section 6.3.1.

6.3.3 RETRAINING FREQUENCY AND REQUIREMENTS

No Stipulation

6.3.4 JOB ROTATION FREQUENCY AND SEQUENCE

No Stipulation

6.3.5 SANCTIONS FOR UNAUTHORIZED ACTIONS

No stipulation

6.3.6 INDEPENDENT CONTRACTOR REQUIREMENTS

The DIP-PKI CM shall ensure that contractor access to its facilities is in accordance with this Certificate Policy. Individuals not security cleared must be under supervision by approved personnel at all times.

The DIP-PKI CM shall ensure that contractor access to its facilities is in accordance with this Certificate Policy. Individuals not security cleared must be under supervision by approved personnel at all times.

6.3.7 DOCUMENTATION SUPPLIED TO PERSONNEL

The DIP-PKI CM shall ensure that all personnel associated with the Certification Manufacture shall be provided access to all documentation relevant to their position. This will include the Certificate Policies and associated Certification Practice Statements relevant to the service, together with any specific supporting documentation, statutes, policies or contracts relevant to the position and role of the personnel.

6.4 AUDIT LOGGING PROCEDURES

6.4.1 TYPES OF EVENTS RECORDED

The DIP-PKI CM shall ensure that in the certificate manufacture operations, Audit logs of all transactions relevant to Certificate creation, Certificate lifecycle management and the operation of trusted systems and services are maintained to provide an audit trail. The event types are at a minimum:

- Messages received from authorised sources requesting an action on the part of the CA.
- All actions taken in response to requests.
- Trusted system installation and any modifications.
- Receipt, servicing and shipping of hardware cryptographic modules.
- Creation and issuance of CRLs.
- All error conditions and anomalies associated with the operation of trusted systems and services.
- Any known or suspected violations of physical security.
- Any known or suspected violations of network and/or trusted system security.
- All CA and trusted application start-up and shutdown.
- All usage of the CA signing key.
- All personnel/role changes for trusted roles.

The Issuing Authority shall ensure the Registration Authority shall record for audit purposes, at minimum, the event types listed below:

Any log on/off attempts by RA operators.

- All messages from authorised sources requesting an action of the RA and the subsequent actions taken by the RA in response to such requests.
  - All messages to the CA requesting an action of the CA and the subsequent action taken by the CA.
  - All physical accesses to RA systems (including components) and RA locations.
  - RA application start-up and shut down.
  - All use of any RA signing key(s).
  - Any suspected or known violations of physical security.
  - Any suspected or known violations of network and system security.
- All checks made for the registration of RA staff.
- All personnel/role changes for trusted roles.

6.4.2 FREQUENCY OF PROCESSING LOG

The DIP-PKI CM shall provide details of audit log processing in the records of role allocation in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority or Auditors acting on its behalf.

6.4.3 RETENTION PERIOD FOR AUDIT LOG

Audit logs are to be retained for a period of no less than seven (7) years.

6.4.4 PROTECTION OF AUDIT LOG

The DIP-PKI CM shall ensure the electronic audit log system must include mechanisms to protect the log files from unauthorised viewing, modification, and deletion. Manual audit information must be protected from unauthorised viewing, modification and destruction.

6.4.5 AUDIT LOG BACKUP PROCEDURES

The DIP-PKI CM shall ensure audit logs and audit summaries are backed up or if in manual form, must be copied.

Such backups must be provided with the same level of security as the originals and must be commensurate with the data contained within them.

6.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

No stipulation

6.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

No stipulation

6.4.8 VULNERABILITY ASSESSMENTS

No stipulation

6.5 RECORDS ARCHIVAL

6.5.1 TYPES OF RECORDS ARCHIVED

The DIP-PKI CM shall ensure the event records and any accompanying data as described in section 6.4.1 of this Certificate Policy are to be archived. Additional information may be retained to ensure compliance with this Certificate Policy and/or legal requirements.

The Issuing Authority shall ensure the Registration Authority retains information provided in support of Certificate application and Revocation requests.

6.5.2 RETENTION PERIOD FOR ARCHIVE

Archived information is to be retained for a period of no less than seven (7) years

6.5.3 PROTECTION OF ARCHIVE

Archives are to be protected from unauthorised viewing, modification, and deletion. Archives are to be adequately protected from environmental threats such as temperature, humidity and magnetism.

Multiple copies of information may be archived.

6.5.4 ARCHIVE BACKUP PROCEDURES

No stipulation.

6.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

No stipulation

6.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

No stipulation

6.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Records of individual transactions may be released upon request by any of the DIP Service Users involved in the transaction, or their recognised representatives.

The DIP-PKI CM shall ensure availability of their archives and that archived information is stored in a readable format during its retention period, even if the DIP-PKI CM operations are interrupted, suspended or terminated.

In the event that the services of the DIP-PKI CM providing Trust Services for or on behalf of the Issuing Authority are to be interrupted, suspended or terminated, the Issuing Authority shall ensure the continued availability of the archive. All requests for access to such archived information shall be sent to the Issuing Authority or to the entity identified by the Issuing Authority prior to terminating its service.

6.6 KEY CHANGEOVER

DIP Service User - a DIP Service User may only replace their Certificate and key pair prior to the expiration of the keys, provided that the current Certificate remains valid and has not been Revoked or Suspended. This key changeover may be initiated by one of the following:

- The DIP Service User (or DIP Connection Provider).
- The Registration Authority.
- The Issuing Authority.

Automated notification of an impending required key changeover is permitted.

DIP Service Users without valid keys will be re-authenticated in the same manner as for an initial registration.

Where a DIP Service Users Certificate has been revoked as a result of suspected or actual non-compliance,

The Issuing Authority that intends to initiate the key changeover process, shall verify that the reasons for non-compliance have been satisfactorily addressed and resolved prior to Certificate Re-issuance.

6.7 COMPROMISE AND DISASTER RECOVERY

6.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

The DIP-PKI CM shall ensure a business continuity plan is in place to protect critical Public Key infrastructure processes from the effect of major compromises, failures or disasters. These shall enable the recovery of all Issuing Authority services. Business continuity plans for DIP Service Users providing Trust Services shall be detailed in the Certification Practice Statement and/or supporting documentation. Plans must be approved by the Issuing Authority or Auditors acting on its behalf.

In the case of comprise of a CA or CA-keys, the Issuing Authority shall as a minimum require the following:

- Immediately cause the suspension of the Certificate Status checking service for all Issued Certificates affected by a compromise, failure or disaster.
    - This will stop any of these Certificates from being accepted by any Relying Party who follows proper Revocation checking procedures
- Suspension of any further Certificate Issuance from the affected CA.

6.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

The DIP-PKI CM shall establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data. Business continuity plans shall be detailed in the Certification Practice Statement and/or supporting documentation. Plans must be approved by the Issuing Authority.

6.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

See part 6.7.1 of this Policy

6.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

The business continuity plan for the Certificate Manufacture shall be designed to deal with any disruption to services and shall ensure managed, progressive recovery of components used to provide the service. A geographically separate alternative backup facility, within the United Kingdom, in order to maintain, at a minimum, for Certificate Status information must be made available.

Any backup facility used for relocation following a disaster shall maintain compliance with this Certificate Policy. The provisions of this Certificate Policy shall be maintained during any relocation/transition.

6.8 CA OR RA TERMINATION

As per contractual agreement

7 TECHNICAL SECURITY CONTROLS

Specific details on technical controls operated for components of the PKI infrastructure must be detailed in the Certification Practice Statement and/or supporting documentation. Controls must be approved by the Issuing Authority.

7.1 KEY PAIR GENERATION AND INSTALLATION

7.1.1 KEY PAIR GENERATION

DIP-PKI Certificate Manufacturer - Issuing Authority keys and CA-key pairs and signing keys shall be generated in a protected environment. CA-Key generation shall be multi-person control using random numbers of such length so as to make it computationally infeasible to regenerate them, even with the knowledge of the when and in which equipment they were generated. See section 7.2.1

Private Keys used in any Issuing Authority and/or Trust Services process that affects the outcome of

- Issued Certificates and Certificate Status Information services (such as signing of Certificate Revocation Lists), will be generated under controlled procedures.
- DIP Service Users conducting such key generation shall provide details of the procedure in the Certification Practice Statement and/or supporting documentation.
- Procedures must be approved by the Issuing Authority or Auditors acting on its behalf.

Keys used for signing shall only be generated by the DIP Service User (Subject) or generated under the direct control of the DIP Service User (Subject).

7.1.2 PRIVATE KEY DELIVERY TO DIP SERVICE USER

Not applicable

7.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUERS

Issuing CAs shall only accept Public Keys from Root Authorities that have been protected during transit and have had the authenticity and integrity of their origin from the Root Authority suitably verified.

The delivery of Public Keys to the Certificate authority shall use PKCS#10 or other equivalent standards compliant cryptographic mechanism or using a process specifically approved by the Certificate Manufacturer. Specific mechanisms must be approved by the Issuing Authority.

7.1.4 PUBLIC KEY DELIVERY TO RELYING PARTIES

Issuing CAs shall ensure that Public Key delivery to Relying Parties is undertaken in such a way as to prevent substitution attacks. This may include working with commercial browsers and platform operators to embed Root Certificate Public Keys into root stores and operating systems. Issuing CA Public Keys may be delivered by the Subscriber in the form of a chain of Certificates or via a Repository operated by the Issuing CA and referenced within the profile of the issued Certificate.

7.1.5 KEY SIZES

The size of the Issuing Authority and supporting CA-Keys shall not be less than 4096 bit modulus for RSA.

The size of DIP Service User's Private keys shall not be less than 2048 bit modulus for RSA.

7.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Public Key exponents shall be of values and lengths that make known attacks (e.g. low exponent attacks) infeasible.

7.1.7 KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)

Certificates Issued under this policy may be used in applications and services as listed below:

- TLS client and server authentication between DIP Service Users and the DIP Messaging Platform
- Digital signing of messages between DIP Service Users and the DIP Messaging Platform
- Where a Certificate has been issued under this policy for the key usage service of non-repudiation the Private Key shall be used solely for the purpose of non-repudiation.

Use of extensions in the Certificate shall be consistent with section 8.1.2 of this Certificate Policy.

7.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

7.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

CA-Keys shall be protected by high assurance physical and logical security controls. They must be stored in, and operated from inside a specific tamper resistant hardware based security module that complies with FIPS140-2 level 3, its equivalents and successors.

Private Keys used in any Issuing Authority and/or Registration Authority process that affects the outcome of Issued Certificates and Certificate Status Information services (such as signing Certificate Revocation Lists), shall be protected by, maintained in, and restricted to, a hardware cryptographic token designed to meet the level of requirements as specified in FIPS 140-2 level 2, or its equivalents and successors.

CA-Keys shall not be available in unprotected form (complete or unencrypted) except in approved cryptographic modules.

7.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

For CA-Keys and keys that affects the outcome of Issued Certificates and Certificate Status Information services, at a minimum, two-person control is required.

7.2.3 PRIVATE KEY ESCROW

This Certificate Policy does not support Key Escrow.

The DCA shall not provide any Key Escrow service

7.2.4 PRIVATE KEY BACKUP

The DIP-PKI CM may backup and archive Private Keys including CA keys

DIP Service Users are responsible for the Back-Up of their own keys.

Key backups shall at a minimum be protected to the standards commensurate with that stipulated for the primary version of the key.

In the case of aggregated backups of keys, (for example, many keys backed-up inside and protected by a single security environment), the backed-up keys must be protected at a level commensurate with that stipulated for the Issuing Authority private signing key.

7.2.5 PRIVATE KEY ARCHIVAL

Stipulated for the issuing Authority’s private signing key.

7.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

If DIP Service User Private Keys are not generated in the DIP-PKI CM cryptographic module, it must be entered into the module via the use of a secure procedure approved by the Issuing Authority. Mechanisms to protect key material and any associated activation data from unauthorised access, modification and use shall be employed.

If DIP Service User Private Keys are not generated in the DIP-PKI CM cryptographic module, it must be entered into the module via the use of a secure procedure approved by the Issuing Authority. Mechanisms to protect key material and any associated activation data from unauthorised access, modification and use shall be employed.

DIP Service Users conducting such key transfer shall provide detail of the procedure in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority. See section 7.1.2.

7.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

See part 7.2.1 of this Policy

7.2.8 METHOD OF ACTIVATING PRIVATE KEY

DIP Service Users who are natural persons must be authenticated to their cryptographic module before the activation of the Private Key. This authentication may be in the form of a PIN, pass-phrase password or other activation data. When deactivated, Private Keys must not be exposed in plaintext form.

7.2.9 METHOD OF DEACTIVATING PRIVATE KEY

No stipulation

7.2.10 METHOD OF DESTROYING PRIVATE KEY

The DIP-PKI CM must ensure Strict controls over destruction of CA-Keys and keys that affect the outcome of Issued Certificates and Certificate Status Information services, must be exercised.

Whether active, expired or archived, the Issuing Authority must approve the destruction of such keys.

7.2.11 CRYPTOGRAPHIC MODULE RATING

See section 7.2.1.

7.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

7.3.1 PUBLIC KEY ARCHIVAL

Public keys shall be archived in accordance with section of this Policy

7.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

Usage periods for key pairs shall be governed by validity periods set in Issued Certificates. These shall have the following maximum values:

- DIP Service User Certificate up to 398 days.
- DIP-PKI CM five (5) years.

7.4 ACTIVATION DATA

7.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

All Issuing Authority supporting DIP-PKI CM CA-Keys and keys that affect the outcome of Issued Certificates and Certificate Status Information services shall have activation data that is unique and unpredictable. The activation data, in conjunction with any other access control, must have an appropriate level of strength for the keys or data to be protected. Where PINs, passwords or passphrases are used, an entity must have the capability to change these at any time.

7.4.2 ACTIVATION DATA PROTECTION

All Issuing Authority supporting DIP-PKI CM CA-Keys and keys that affect the outcome of Issued Certificates and Certificate Status Information services shall have mechanisms for the protection of activation data which is appropriate to the Keys being protected.

Details of protection shall be provided in the Certification Practice Statement and/or supporting documentation. Procedures must be approved by the Issuing Authority.

7.4.3 OTHER ASPECTS OF ACTIVATION DATA

Not applicable in this Policy

7.5 COMPUTER SECURITY CONTROLS

7.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The DIP-PKI CM shall implement security measures that have been identified through a threat assessment exercise and must cover the following functionality where appropriate:

- Access control to trust services and PKI roles.
- Enforced separation of duties for PKI roles.
- Identification and authentication of PKI roles and associated identities.
- Use of cryptography for session communication and database security.
- Archival of DIP Service User history and audit data.
- Audit of security related events.
- Trusted path for identification of PKI roles and associated identities.
- Recovery mechanisms for keys of PKI DIP Service Users providing trust services.

This functionality may be provided by the operating system, or through a combination of operating system, DCA software, and physical safeguards.

The DIP-PKI CM shall document procedures in the Certification Practice Statement and/or supporting documentation. Procedures shall at a minimum include logging and audit requirements for processes related to initialisation, resetting, shutdown or reconfiguration of Certificate Authorities and any services that affect the outcome of Issued Certificates and Certificate Status Information.

7.5.2 COMPUTER SECURITY RATING

The DIP-PKI CM may use system components that do not possess a formal computer security rating provided that all requirements of this Certificate Policy are satisfied.

Any hardware security module or device holding CA Keys must comply with the requirements of 7.2.1 of this Certificate Policy.

Where specific computer security rating requirements are specified in this Certificate Policy, details of relevant components and how they satisfy the requirements must be provided in the Certification Practice Statement and/or supporting documentation.

7.6 LIFE CYCLE TECHNICAL CONTROLS

7.6.1 SYSTEM DEVELOPMENT CONTROLS

The development of software that implements the DIP-PKI CM functionality shall as a minimum be performed in a controlled environment that, together with at least one of the following approaches, shall protect against the insertion of malicious logic.

- The system developer shall have a quality system compliant with international standards or;
- The system developer shall have a quality system available for inspection and approval by the Issuing Authority.

7.6.2 SECURITY MANAGEMENT CONTROLS

The configuration of systems operated by the DIP-PKI CM as well as any modifications, upgrades and enhancements must be documented and controlled. There must be a method of detecting unauthorised modification or configuration of the software supporting Trust Services. The DIP-PKI CM shall ensure that it has a configuration management process in place to support the evolution of the systems under its control.

Details of security management systems shall be provided in the dip-PKI-CPS and/or supporting documentation which must be approved by the Issuing Authority.

7.6.3 LIFE CYCLE SECURITY CONTROLS

See part 7.6.2 of this Policy

7.7 NETWORK SECURITY CONTROLS

The DIP-PKI CM systems must be protected from attack through any open or general-purpose network with which they are connected. Such protection must be provided and configured to allow only the minimal set of functions, protocols and commands required for the operation of the Trust Service.

The DIP-PKI CM shall detail the standards procedures and controls for network security in the Certification Practice Statement and/or supporting documentation which must be approved by the Issuing Authority or Auditors acting on its behalf.

7.8 TIME-STAMPING

The DIP-PKI CM shall implement time recording for all Certificate and other related activities that require recorded time. A synchronised and controlled time source shall be used.

The DIP-PKI CM shall detail the time source used and mechanisms for its control in the Certification Practice Statement and/or supporting documentation which must be approved by the Issuing Authority or Auditors acting on its behalf.

8 CERTIFICATE, CRL, AND OCSP PROFILES

8.1 CERTIFICATE PROFILE

Certificate Profiles are under the direct control of the DIP Manager. The DCA shall only issue Certificates in accordance with the Certificate Profiles in the CoCo section 8.7

8.1.1 VERSION NUMBER(S)

Only Certificates that conform to X.509 Version 3 and IETF RFC 5280 can be used.

8.1.2 CERTIFICATE EXTENSIONS

All End Entity PKI software must correctly process the extensions identified in sections 4.2.1 and 4.2.2 of the IETF RFC 5280 Certificate Profile Specification. The following are common Certificate extensions:

- The Basic Constraints extension is set to TRUE for CA-certificates only; its use is critical specifying that it is a CA-certificate. DIP Service User end entity Certificates have the value set to FALSE.

- The Certificate Policies extension is mandatory and shall contain an OID indicating the use of this policy. The Certificate Policy Qualifier Info extension shall be used to direct end-entities to where this policy and other relevant information may be found.
- Where CRLs are used to produce Certificate Status information, the CRL Distribution Point extension is mandatory, and shall identify a location where the latest CRL Issued by the Issuing Authority can be obtained.

8.1.3 ALGORITHM OBJECT IDENTIFIERS

No stipulation

8.1.4 NAME FORMS

The use of all name forms shall be consistent with section 4.1 of this Policy. Name forms shall be approved by the Issuing Authority.

8.1.5 NAME CONSTRAINTS

No stipulation

8.1.6 CERTIFICATE STATEMENTS OBJECT IDENTIFIER

The use of all name forms shall be consistent with section 8.1 of this Policy. Name forms shall be approved by the Issuing Authority.

8.1.7 USAGE OF STATEMENTS CONSTRAINTS EXTENSION

No stipulation

8.1.8 STATEMENTS QUALIFIERS SYNTAX AND SEMANTICS

No stipulation

8.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

No

8.2 CRL PROFILE

8.2.1 VERSION NUMBER(S)

Only Certificate Revocation Lists conforming to X.509 version 2 and IETF RFC 5280 may be issued.

An alternative to CRLs is permitted. The Issuing Authority may allow for provision of an on-line Certificate Status checking service, which meets the requirements in this DIP-PKI CP

8.2.2 CRL AND CRL ENTRY EXTENSIONS

No stipulation

8.3 OCSP PROFILE

8.3.1 VERSION NUMBER(S)

OCSP and other forms of Certificate Status Information provision are permitted.

Repositories shall detail the mechanisms for on line Certificate Status Information provision in the DIP-PKI CP and/or supporting documentation which must be approved by the Issuing Authority or Auditors acting on its behalf.

8.3.2 OCSP EXTENSIONS

No stipulation

9 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

9.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The details for assessment are specified in contractual arrangements between the Issuing Authority and the DIP-PKI CM.

The audit must be sufficient to demonstrate to the Issuing Authority that the services comply with this DIP-PKI CP and any supporting policy documents applicable to their services.

For the DIP-PKI CM, assessment shall be against prescribed criteria defined by the Policy Authority and shall be conducted not less than annually

9.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The suitability of assessors to perform assessment of the Issuing Authority and its associated Registration Authorities is decided by the Policy Authority.

Approved Auditors may include internal auditing resources of DIP Service Users, subject to the approval of the Policy Authority.

For DIP-PKI CM audit shall be conducted by a Policy Authority approved third-party auditor.

9.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The acceptability of auditors is decided by the Policy Authority.

9.4 TOPICS COVERED BY ASSESSMENT

An Audit is required to ensure the DCA providing Trust Services, i.e. the DIP-PKI CM, is operating in accordance with its DIP-PKI CPS, this DIP-PKI CP and any declared assurance or approval schemes under which Trust Services are operated.

The Audit will address all aspects of the Trust Service operations (whether they directly or indirectly influence compliance with the Certification Practice Statement) to ensure overall standards of operation are commensurate with this DIP-PKI CP.

9.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

For compliance audits of the DIP-PKI CM, where significant exceptions or deficiencies are identified, the Issuing Authority will inform the Policy Authority and determine the action to be taken.   A remedial action plan will be developed with input from the auditor. The Policy Authority has overall responsibility to ensure implementation of the action plan. If an immediate threat to the security or integrity of the PKI services is identified a corrective action plan which may include suspension or termination of noncompliant services will be developed, approved by the Policy Authority and implemented by the Issuing Authority. For lesser exceptions or deficiencies, the Issuing Authority will determine the course of action to be taken.

9.6 COMMUNICATION OF RESULTS

Where compliance with third party assurance or approval schemes under which Trust Services are operated has been audited, approval status shall be made publicly available by the DIP Service Users providing Trust Services if required under the scheme.

In the event of identification of material non-compliance with this DIP-PKI CP, the Issuing Authority shall make available to DIP Service Users and Relying Parties details of action to be taken as a result of the deficiency and any remedial action required to be taken.

10 GLOSSARY

Terms used in this Policy.

Activation Data	Private data, other than keys, that are required to access cryptographic modules.
Asymmetric Cryptosystem	A system which generates and employs a secure key consisting of a Private Key for creating a Digital Signature and a Public Key to verify a Digital Signature. Also known as Public Key Cryptography.
Authentication	The process of establishing that individuals, organisations, or devices are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organisation applying for or seeking access to something under a certain name is, in fact, the proper individual or organisation. Authentication can also refer to a security service that provides assurances that individuals, organisations, or things are who or what they claim to be or that a Message or other data originated from a specific individual, organisation, or device. Thus, it is said that a Digital Signature of a Message authenticates the Message's sender.

CAA	Certification Authority Authorisation (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorised to issue certificates for that domain.
Certificate	A collection of data that at a minimum: Identifies the Issuing Authority Names or identifies its Subject Contains the Subject's Public Key Identifies the operational period of Certificate Bears the Digital Signature of the Issuing Authority Also known as Digital Certificate
DIP Certificate Authority (DCA) DIP Certificate Authority (DCA) System	The software and hardware system used by the Issuing Authority or it's designated Certificate Manufacturer to issue and manage the full lifecycle of certificates.
DCA Certificate (DCA-Certificate)	See Issuing Authority Certificate.
DCA Key (CA- Key)	The Private Key used by the CA for signing Certificates and other objects.
Certificate Discovery	The process of obtaining a DIP Service Users certificate. Typically from the DIP User Portal.
DIP Certificate Manufacturer	The entity providing certificate management services and facilities for an Issuing Authority.
DIP Certificate Statements (CP)	A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. A Certificate Statements may be employed by a Certificate user to help in deciding whether a Certificate (and the binding therein), is sufficiently trustworthy for a particular purpose. A CP may be supported by one or more CPSs.
DIP Certificate Profile	Defines the usage of the Certificate and is formally approved by the Statements Authority and the Issuing Authority.

Certificate Revocation List (CRL)	A list maintained by, or on behalf of, an Issuing Authority of the Certificates that it has issued, that have been Revoked or Suspended before the expiry stated in the Certificate.
Certificate Status Discovery	The process of ascertaining the Operational Status of a Certificate. Typically via a controlled mechanism from a Repository. Also known as Certificate Status Checking
Certificate Status Information	Information that indicates whether Certificates have been Revoked or Suspended; commonly provided via Certificate Revocation Lists, or individually through specific online enquiries (e.g. OCSP).
Certificate Service Provider (CSP)	See also DIP Service User. The term CSP is used in connection with the EU Electronic Signatures Directive and Supporting ETSI Standards.
Certificate User	See Relying Party
DCA	See Issuing Authority
Certification Path	A logical and ordered sequence of Certificates which, together with the Public Key of the initial object in the Certification Path, can be processed to obtain that of the final object in the Certification Path.
DIP CPS	A statement of the procedures and practices employed in the issuing, managing, revoking, and renewing of certificates. A CPS may support of one or more Certificate Policies.
Confirm	Ascertain through appropriate inquiry and investigation.

Content Commitment	An action whereby a signer of a message commits to the content being signed by them. This term is sometimes used synonymously with NonRepudiation, however, in any specific context the detailed definition may result in its legal standing differing from that of Non-Repudiation. See also Non-Repudiation
Corresponding Private Key	Given a public key taken from a key pair, the corresponding private key is the private key from that same key pair, (and vice-versa for corresponding public key).
Cross-certificate	A Certificate used to establish a trust relationship between two Issuing Authorities.
Digital Certificate	See Certificate
Digital Signature	The result of a transformation of a message by means of a cryptographic system and a Hash Function, using keys such that a person who has the initial Message can determine: Whether the transformation was created using the Private Key that corresponds to the signer's Public Key, and Whether the initial Message has been altered since the transformation was made.

	such that a person who has the initial Message can determine: Whether the transformation was created using the Private Key that corresponds to the signer's Public Key, and Whether the initial Message has been altered since the transformation was made.

End-Entity	Those using Digital Certificates. See DIP Service User and Relying Party
Hash Function	An algorithm mapping or translating one sequence of bits into another, generally smaller, set (the Hash or Message Digest) such that: A Message yields the same Hash result every time the algorithm is executed using the same Message as input; It is computationally infeasible that a Message can be derived or reconstituted from the Hash result provided by the algorithm; and It is computationally infeasible that two Messages can be found that produce the same hash result using the algorithm
Hash	The output produced by a Hash Function upon processing a Message (see also Message Digest).
High Security Zone	An area to which access is controlled through an entry point and is limited to authorised, appropriately screened personnel and properly escorted visitors. High-Security Zones should be accessible only from Security Zones, and are separated from Security Zones and Operations Zones by a perimeter built to the specifications recommended in a threat risk assessment. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Hold a Private Key	To use or to be able to use a Private Key.
Incorporate by Reference	Make one Message a part of another Message by:- Identifying the Message to be incorporated; Providing information which enables the Receiving Party to access and obtain the incorporated Message in its entirety; and Expressing the intention that it be part of the incorporating Message. The incorporated Message shall have the same effect as if it had been fully stated in the incorporating Message to the extent permitted by law.

Issuance (Issue a Certificate)	The acts of an Issuing Authority in creating a Certificate which is bound to a DIP Service User. The process requires Authentication of the DIP Service User and/or Subject.
Issuing Authority	By definition, an Issuing Authority is the entity listed in the issuer field of a Digital Certificate. The Issuing Authority may obtain benefit in return for taking on the risks associated with transactions secured by Digital Certificates, for example, risk of fraud. The Issuing Authority has the responsibility for deciding who may be issued with a Certificate carrying its name.
Issuing Authority Certificate	A Certificate for an Issuing Authority's Public Key, and for use in signing Certificates created by certificate authority software under its control.
Key Pair	In an Asymmetric Cryptosystem - a Private Key and its mathematically related Public Key having the property that the Public Key can verify a Digital Signature that the Private Key creates.
Local Registration Authority (LRA)	See Registration Authority
Message	A digital representation of information.
Message Digest	The output produced by a Hash Function upon processing a Message.
Message Integrity	The assurance of the unaltered status of a Message.
Non-repudiation	Strong and substantial evidence of the identity of the Signer of a Message and of Message Integrity, sufficient to prevent a party from successfully denying the original submission or delivery of the Message and the integrity of its contents. See also Content Commitment
Notify	Communicate or make available information to another person as required under the circumstances
Online Certificate Status Protocol	A network protocol used to ascertain the current validity status of a Certificate.

(OCSP)	
Operational Period of Certificate	The Operational Period of a Certificate begins on the date and time it is issued by an Issuing Authority (or on a later date and time certain if stated in the Certificate), and ends at the completion of its Validity Period unless it is earlier Revoked or Suspended.
Operations Zone	An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a threat risk assessment, and should preferably be accessible from a Reception Zone.
DIP Service User	An individual or organisation that plays a role within a given a PKI, typically as a DIP Service User, Relying Party, CA, RA or Certificate Manufacturer. Entities other than DIP Service Users, Subjects and Relying Parties (i.e. not End Entities) may also be known as a Trust Service Provider (TSP) or a Certificate Service Provider (CSP).
Public Key Infrastructure (PKI)	A system of Digital Certificates, Certificate Authorities, and other components that verify and authenticate the validity of parties involved in electronic transactions.
PKI Disclosure Statement (PDS)	An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing, summarising and emphasizing information normally covered in detail by associated CP and/or CPS documents. A PDS is not intended to replace a CP or CPS.
Statements Qualifier	Statements dependent information that may accompany a CP identifier in an X.509 certificate.

Post-Authorisation	A Registration Authority process whereby Certificate Applicants have their identity authenticated during the Certificate application process. Also know as Post-Authentication
Pre-Authorisation	A Registration Authority process whereby Certificate Applicants have their identity authenticated prior to submitting a Certificate application. Also know as Pre-Authentication
Private Key	The private part of an asymmetric key pair used for public key encryption techniques. The Private Key is typically used for signing Digital Signatures or for decrypting Messages.
Public Key	The public part of an asymmetric key pair used for public key encryption techniques. The public key is typically used for verifying digital signatures or to encrypt messages to the owner of the private key.
Public Key Cryptography	See Asymmetric Cryptosystem
Public-access Zone	An area in which there is no personnel access control. Generally surrounds or forms part of a security facility. Examples include the grounds surrounding a building, and public corridors and elevator lobbies in multipleoccupancy buildings. Boundary designators such as signs and direct or remote surveillance may be used to discourage unauthorised activity.
Reception Zone	The entry to a facility where the initial contact between the public and the facility occurs, where services are provided, information is exchanged and access to restricted (Operations, Security and High-security) zones is controlled. To varying degrees, activity in a Reception Zone is monitored by the personnel who work there, by other personnel or by security staff. Access by the public may be limited to specific times of the day or for specific reasons. Entry beyond the Reception Zone is indicated by a recognisable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.

Registration Authority (RA)	An entity that is authorised or licensed by an Issuing Authority to carry out the practices and procedures for one or more of the following functions: the identification and authentication of certificate applicants; the approval or rejection of Certificate applications; initiating Certificate Revocations or Suspensions under certain circumstances; processing requests to revoke or suspend Certificates; approving or rejecting requests by for the Renewal or Re-Key of certificates. An RA does not have responsibility for signing or issuing Certificates or Certificate Status Information.
Registration Authority Operator (RAO)	Registration Authority staff member with approvals to conduct a full set of Certificate management functions
Relying Party	A recipient of a Certificate who acts in reliance on that certificate and/or any Digital Signatures verified using that Certificate. Also known as Certificate User.
Relying Party Agreement (RPA)	An agreement between an Issuing Authority and a Relying Party that typically establishes the rights and obligations between those parties regarding the verification of Digital Signatures or other uses of Certificates. Also known as Relying Party Charter.
Repository	The entity providing community-wide accessible mechanisms by which DIP Service Users can obtain Certificate or Certificate Status information to validate Certificates, and obtain Statements and other controlling information for the PKI.
Re-Key a Certificate	The process by which an existing Certificate has its Public Key value changed by issuing a new certificate with a different (usually new) Public Key. Notably all characteristics relating to the Subject of the Certificate remain unchanged unless Re-Key is combined with a Renewal or Issuance of a new Certificate.
Renewal (Renew a Certificate)	The process by which an existing Certificate that is bound to a DIP Service User is replaced by issuing a new Certificate to that DIP Service User. Typically

	this is based upon the validity of the existing Certificate. This process normally involves a Re-Key.
Revocation (Revoke a Certificate)	Permanently end the Operational Period of a Certificate from a specified time.
Revocation Information	Information required before enacting a Certificate Revocation (or Suspension). It must include evidence of the authenticity of the requestor.
Security Zone	An area to which access is limited to authorised personnel and to authorised and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Signer	A person who creates a Digital Signature for a Message.
Subject	The entity named or identified in a certificate issued to a person, organisation or device, and who holds a Private Key corresponding to the Public Key listed in the Certificate. A Subject may also be a DIP Service User. A Subject must always be either: a DIP Service User or formally bound under the jurisdiction of a DIP Service User
DIP Service User	An entity that contracts with an Issuing Authority for the issuance of Certificates. The DIP Service User bears ultimate responsibility for the use of the Private Key associated with the Certificate. The DIP Service User may be a Subject acting on its own behalf.
DIP Service User Agreement	An agreement between an Issuing Authority and a DIP Service User that establishes the rights and
Time-stamping Authority	The Trust Service Provider operating, controlling and issuing time-stamps for use by other entities.
Trusted Role	A function in the operation of a Trust Service, CA, RA or PKI that. Can influence the status of issued digital certificates.

	Is able to affect the security or functionality of components that enforce security of the service.
Trust Infrastructure	See Public Key Infrastructure
Trust Service	A trust-enhancing service offered or performed by a Trust Service Provider that supports the assurance, integrity or security of electronically executed activities, (e.g. Time-stamping, notarisation, watermarking etc.) The service offered or performed by an Issuing Authority, Registration Authority, Certificate Manufacturer or other trusted intermediary relating to the issuance and control of Digital Certificates, (e.g. manufacture, Issuance, Revocation, publication, registration, validity-checking or defining Statements).
Trust Service Provider (TSP)	An entity that acts as a supplier of Trust Services. See also DIP Service User. Also known as Certificate Service Provider (CSP)
Trustworthy System	Computer hardware, software and procedures that:
	Are adequately secure from intrusion and misuse; Provide an adequate level of availability, reliability and correctness of operation; Are adequately suited to performing their intended functions; and Adhere to generally accepted security principles.
Validation	See Authentication
Validity Period	The period that is defined within a Certificate, during which that Certificate is intended to be valid. See also Operational Period responsibilities of the parties regarding the issuance and management of Certificates and Associated Private Keys.
Suspension (Suspend a Certificate)	Temporarily make a Certificate non-Operational from a specified time for a period up to the end of its Validity Period

Time-stamp	To create a notation that indicates, at a minimum, the correct date and time of an action or activity and the identity of the entity that created the notation; or such a notation is appended, attached or referenced as a part of a data structure. Time-stamps may, but do not require derivation of chronological data from a secure time source and/or use cryptographic techniques to persevere the integrity of the Time-stamp.
Time-stamping Authority	The Trust Service Provider operating, controlling and issuing time-stamps for use by other entities.
Trusted Role	A function in the operation of a Trust Service, CA, RA or PKI that. Can influence the status of issued digital certificates. Is able to affect the security or functionality of components that enforce security of the service.
Trust Infrastructure	See Public Key Infrastructure
Trust Service	A trust-enhancing service offered or performed by a Trust Service Provider that supports the assurance, integrity or security of electronically executed activities, (e.g. Time-stamping, notarisation, watermarking etc.) The service offered or performed by an Issuing Authority, Registration Authority, Certificate Manufacturer or other trusted intermediary relating to the issuance and control of Digital Certificates, (e.g. manufacture, Issuance, Revocation, publication, registration, validity-checking or defining Statements).
Trust Service Provider (TSP)	An entity that acts as a supplier of Trust Services. See also DIP Service User. Also known as Certificate Service Provider (CSP)
Trustworthy System	Computer hardware, software and procedures that: Are adequately secure from intrusion and misuse; Provide an adequate level of availability, reliability and correctness of operation; Are adequately suited to performing their intended functions; and Adhere to generally accepted security principles.
Validation	See Authentication

Validity Period	The period that is defined within a Certificate, during which that Certificate is intended to be valid. See also Operational Period
Verify (a Digital Signature and/or Message Integrity)	In relation to a given Digital Signature, Message and Public Key, to determine accurately: That the Digital Signature was created during the Operational Period of a Valid Certificate by the Private Key corresponding to the Public Key listed in the Certificate; and That the Message has not been altered since its Digital Signature was created.
Vettor	Registration Authority staff member with approvals to conduct a limited set of Certificate management functions