**DSD002 Annex Three – The DIP-PKI (Public Key Infrastructure) Policy**

**Amendment Record**

| Version | Date | Description of Change | Approval Reference |
| --- | --- | --- | --- |
| 0.1 |  | Issue 101 Consultation | - |
| 0.2 |  | Issue 101 Report | - |
| 0.3 |  | Shared with Ofgem |  |
| 0.4 |  | P474 |  |

**Contents**

[1 Overview 5](#_Toc169521325)

[1.1 Scope and purpose 5](#_Toc169521326)

[1 Key organisations 6](#_Toc169521327)

[1.1 DIP Manager 6](#_Toc169521328)

[1.2 DIP Verification Service Provider 7](#_Toc169521329)

[1.3 DIP Users 7](#_Toc169521330)

[1.4 DIP Connection Providers (DCP) 7](#_Toc169521331)

[1.5 Replying Parties 7](#_Toc169521332)

[2 DIP Repositories and responsibilities 9](#_Toc169521333)

[2.1 DIP Repositories 9](#_Toc169521334)

[2.2 DIP-PKI Repository responsibilities 9](#_Toc169521335)

[3 Identification and Authentication 10](#_Toc169521336)

[3.1 Naming 10](#_Toc169521337)

[3.2 Identification and authentication for routine re-key 10](#_Toc169521338)

[4 Certificate lifecycle Operational requirements 11](#_Toc169521339)

[4.1 Digital Certificate application processing 11](#_Toc169521340)

[4.2 Digital Certificate Issuance 11](#_Toc169521341)

[4.3 Digital Certificate acceptance 12](#_Toc169521342)

[4.4 Key Pair and Digital Certificate usage 12](#_Toc169521343)

[4.5 Digital Certificate renewal 12](#_Toc169521344)

[4.6 Digital Certificate voluntary revocation 12](#_Toc169521345)

[4.7 Circumstances for revoking a Digital Certificate 13](#_Toc169521346)

[4.8 CRL issuance frequency 13](#_Toc169521347)

[4.9 On-line revocation/status checking 14](#_Toc169521348)

[4.10 Actions in the event of a Private Key compromise 15](#_Toc169521349)

[4.11 End of subscription 15](#_Toc169521350)

[4.12 Key escrow and recovery statements and practices 15](#_Toc169521351)

[5 Facility, management, and operational controls 16](#_Toc169521352)

[5.1 Overview 16](#_Toc169521353)

[5.2 Physical Controls 16](#_Toc169521354)

[5.3 Procedural controls 17](#_Toc169521355)

[5.4 Personnel controls 18](#_Toc169521356)

[5.5 Audit Logging Procedures 18](#_Toc169521357)

[5.6 The IA shall ensure the RA shall record for audit purposes, at minimum, the event types listed below: 19](#_Toc169521358)

[5.7 Record archiving 20](#_Toc169521359)

[5.8 Key changeover 20](#_Toc169521360)

[5.9 Compromise and disaster recovery 21](#_Toc169521361)

[6 Technical Security Controls 22](#_Toc169521362)

[6.1 Key pair generation and installation 22](#_Toc169521363)

[6.2 Key sizes and parameters 22](#_Toc169521364)

[6.3 Key usage purposes (as per x.509 v3 key usage field) 23](#_Toc169521365)

[6.4 Private Key protection and cryptographic module engineering controls 23](#_Toc169521366)

[6.5 Private Key transfer into or from a cryptographic module 23](#_Toc169521367)

[6.6 Method of activating Private Keys 24](#_Toc169521368)

[6.7 Method of destroying private key 24](#_Toc169521369)

[6.8 Other aspects of key pair management 24](#_Toc169521370)

[6.9 Activation Data 24](#_Toc169521371)

[6.10 Computer security controls 24](#_Toc169521372)

[6.11 Life Cycle Technical Controls 25](#_Toc169521373)

[6.12 Network Security Controls 26](#_Toc169521374)

[7 Certificate, CRL, and OCSP Profiles 27](#_Toc169521375)

[7.1 Certificate Profile 27](#_Toc169521376)

[7.2 CRL Profile 27](#_Toc169521377)

[7.3 OCSP Profile 27](#_Toc169521378)

[8 Compliance Audit and other assessments 28](#_Toc169521379)

[8.1 Frequency or circumstances of assessment 28](#_Toc169521380)

[8.2 Identity/qualifications of assessor 28](#_Toc169521381)

[8.3 Assessor's relationship to assessed entity 28](#_Toc169521382)

[8.4 Topics covered by assessment 28](#_Toc169521383)

[8.5 Actions taken as a result of deficiency 28](#_Toc169521384)

[8.6 Communication of results 29](#_Toc169521385)

# Overview

## Scope and purpose

This Annex to DSD002 ‘DIP Connection and Operation’ has been published as the DIP-PKI Policy to set out the requirements for the DIP-PKI. It sets out the rules and applicability of a Digital Certificate to the DIP.

This DIP-PKI Policy defines a PKI and, in conjunction with the PKI Disclosure Statement (if published), specifies:

1. who can participate in the PKI defined by this DIP-PKI Policy;
2. the primary rights, obligations and liabilities of the parties governed by this DIP-PKI Policy;
3. the purposes for which Digital Certificates issued under this Policy may be used; and
4. the minimum requirements to be observed in the issuance, management, usage and reliance on Digital Certificates.

The DIP Manager shall operate the DIP-PKI in accordance with this DIP-PKI Policy.

This DIP-PKI Policy is structured in accordance with the guidelines in IETF RFC 3647.

# Key organisations

## DIP Manager

The DIP Manager is responsible for approving rights, obligations and all other terms and conditions contained in this DIP-PKI Policy, and any questions relating to this DIP-PKI Policy shall be directed to them.

For the purposes of the DIP-PKI Policy the DIP Manager shall assume multiple roles that in other PKI environments may be undertaken by multiple entities. The roles the DIP Manager undertakes are:

1. DIP Certificate Authority (DCA);
2. Issuing Authority (IA);
3. Trust Service Provider;
4. Policy Authority;
5. Registration authority; and
6. Repository Manager.

The DIP Manager’s responsibilities include:

1. being the entity listed in the Issuer field of a Certificate;
2. being the ‘owner’ of the DIP;
3. determining whether DIP Users (including checks on their eligibility) shall be issued with a Digital Certificate carrying its name as the Issuer;
4. control over the request, issuance, management, revocation, suspension and usage of Digital Certificates issued pursuant to this DIP-PKI Policy, and the provisions to deal with such requests;
5. holding data in support of PKI operations, including policy and related documentation, Digital Certificates and Digital Certificate status information;
6. providing a community-wide accessible mechanism by which (primarily) DIP Users and Relying Parties can obtain and validate information on Digital Certificates;
7. issuing Certificate Profiles (see Annex 2) that define Digital Certificate usage.

The DIP Manager shall ensure that Digital Certificates are only issued for the purposes of:

1. the creation, sending, receiving and processing of communication within the DIP environments in accordance with the DIP Rules;
2. Symmetric key generation (Digital Signature, Key Agreement);
3. TLS Communication (Digital Signature, Key Agreement, TLS Web Client Authentication, TLS Web Server Authentication);
4. Authentication and Non-Repudiation (Digital Signature, Non-Repudiation, Key); and
5. Encipherment and Data Encipherment (Key Agreement, TLS web client authentication, and TLS web server authentication).

The DIP Manager determines the suitability of any DIP-PKI Certification Practice Statement (CPS) operating under this DIP-PKI Policy. The DIP Manager shall review DIP-PKI CPSs as part of the DIP Assurance Strategy and shall, where the DIP Strategy requires, be subject to audit by the DIP Manager.

For purposes of this DIP-PKI Policy and operating model, there will be a single Registration Authority – the DIP Manager.

## DIP Verification Service Provider

The DIP Verification Service Provider shall be the DIP Certificate Manufacturer (DIP CM).

The DIP CM provides the infrastructure and operational services for the DIP Manager in relation to the manufacture of Digital Certificates.

The DIP CM has no authority to make decisions on the issuance of Certificates, or other aspects of Digital Certificate management outside the Certificate Manufacturing process.

The DIP CM operates under the direction of the IA and must demonstrate compliance with this Policy via the Certification Practice Statement (CPS).

## DIP Users

In respect to the DIP-PKI Policy and environment, DIP Users bear responsibility for the use and security of the Private Key associated with a Digital Certificate.

## DIP Connection Providers (DCP)

DIP Users may use DCPs to represent them as an authorised representative. A DIP User using a DCP is ultimately responsible for ensuring the DCP complies with the DIP-PKI Policy.

In all cases, the DIP User is responsible for compliance with the DIP-PKI Policy and all other obligations applicable to it and the DCP.

## Replying Parties

Entities that are using a Digital Certificate to authenticate another Digital Certificate subscriber named in the Digital Certificate.

In the context of the DIP, every Digital Certificate subscriber is also a Relying Party at some point in the process of exchanging messages with the DIP and DIP Service Users.

# DIP Repositories and responsibilities

## DIP Repositories

The DCA and the DIP CM shall have their own DIP-PKI Repositories.

The DIP CM’s DIP-PKI Repository stores the following information:

1. all copies of issued DIP-PKI Operator Root CA Certificates; and
2. Digital Certificate status and validity meta-data for each DCA Digital Certificate.

The DCA’s DIP-PKI Repository stores the following information:

1. all copies of Digital Certificates issued by the DCA;
2. certificate status and validity meta-data for each Digital Certificate;
3. the latest version of the DIP-PKI Certificate Revocation List (CRL);
4. all copies of issued DCA Certificates See CoCo section 6 for details.

## DIP-PKI Repository responsibilities

The DCA Shall ensure that:

1. each Digital Certificate is promptly accepted by a DIP User when issued;
2. each Digital Certificate is lodged in the applicable DIP-PKI Repository promptly on being issued; abd
3. the DIP-PKI CRL is lodged in the DIP-PKI Repository within the timescales required by this DIP-PKI Policy.

All DIP-PKI Repositories are subject to access controls using usernames and passwords with only authorised personnel having access to DIP-PKI Repositories.

# Identification and Authentication

## Naming

The DIP Manager shall ensure that the name of the entity that is the subject of each Digital Certificate is in accordance with the relevant Certificate Profile (see Annex 2).

The anonymity or pseudonymity of DIP Users is not supported by the DIP-PKI Policy or the DIP Rules.

## Identification and authentication for routine re-key

This DIP-PKI Policy does not support Digital Certificate re-key and therefore will not provide a Re-Key Service, and by implication does not provide provision for identification and authentication for a Certificate re-key after revocation.

# Certificate lifecycle Operational requirements

## Digital Certificate application processing

All CSRs will be processed within seven seconds of receipt of request.

Where a CSR satisfies the requirements set out in DSD002 Annex 2 ‘Detailed DIP Operational Requirements’, the DCA shall issue the required Digital Certificate.

Where any CSR fails to satisfy the requirements, the DIP Manager shall reject the CSR and refuse to issue the associated Digital Certificate. The DCA shall inform the CSR submitter why their CSR was rejected.

## Digital Certificate Issuance

The DCA shall issue a Digital Certificate only:

1. in accordance with the provision in this DPI-PKI Policy and the DIP Rules; or
2. in response to a CSR made by an eligible DIP User.

The DCA shall ensure that:

1. each Digital Certificate contains information that it has verified to be correct and complete; and
2. each Digital Certificate contains information consistent with the information in the Certificate Digital Signature Digital Certificate.

A DIP-PKI Digital Certificate may only be issued by the DCA and signed using a DCA Private Key.

The DCA shall not issue:

1. a Digital Certificate using an Operator Root CA Certificate Private Key after the expiry of the validity period of an Operator Root CA Certificate containing the Public Key associated with that Private Key;
2. a DIP-PKI Digital Certificate using a CA Private Key after the expiry of the validity period of a CA Certificate containing the Public Key associated with that Private Key; or
3. any Digital Certificate containing a Public Key where it is aware that the Public Key is the same as the Public Key contained in any other Digital Certificate that was previously issued by it.

The DCA shall inform the CSR submitter of the issuance/rejection of a Digital Certificate that they have requested in accordance with the DIP Rules.

## Digital Certificate acceptance

A Digital Certificate which has been issued by the DCA shall be treated as valid for any purpose covered by this DIP-PKI 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 User.

## Key Pair and Digital Certificate usage

Provision for restrictions on the use by DIP Users of Private Keys in respect of Digital Certificates is made in this DPI-PKI Policy.

Relying Party obligations are set out in DSD002 Annex 2 ‘Detailed DIP Operational Requirements’.

## Digital Certificate renewal

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

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

Every Digital Certificate issued by the CA for the DIP will have a validity period of 398 days. Prior to expiry, a DIP User should generate a new CSR and get it signed via the DIP Portal.

As all requests for signing come through the DIP Portal, the DIP will notify (see DSD002 Annex 2 ‘Detailed DIP Operational Requirements’) the DIP User that a Digital Certificate is about to expire, and therefore that they should generate a new CSR and get it signed via the DIP.

The new certificate will start from the date the CSR 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.

## Digital Certificate voluntary revocation

DIP Users can submit a Certificate Revocation Request (CRR) to revoke Digital Certificates using the DIP Portal as follows:

1. from within the DIP, the DIP User navigates to the Digital Certificates page, which will show current certificates;
2. under the Digital Certificate actions option, they can choose ‘revoke’. A reason for revocation must be selected from a list of possible reasons;
3. on submission of the reason, the DIP will use the organisation’s API credentials and mTLS Digital Certificate, to ask the DIP Manager to revoke the certificate; and
4. the DIP will inform the DIP User Administrator that the certificate is successfully revoked once approved by the DIP Manager.

Once revoked**,** the Digital Certificate will no longer be valid when calling the DIP.

## Circumstances for revoking a Digital Certificate

A DIP Service User shall submit a CRR through the DIP in accordance with this DIP-PKI Policy:

1. immediately upon becoming aware that the Digital Certificate has been compromised, or is suspected of having been compromised; and
2. immediately upon ceasing to be an eligible DIP User in respect of that Digital Certificate.

A Digital Certificate must be Revoked:

1. when any of the information in the Digital Certificate is known or suspected to be inaccurate;
2. upon suspected or known compromise of the Private Key associated with the Digital Certificate; or
3. upon suspected or known compromise of the media holding the Private Key associated with the Digital Certificate.

The DCA may revoke a Digital Certificate if a DIP User fails to comply with any obligations set out in the DIP Rules, including within the this DIP-PKI Policy.

Any approved request for revocation will be reflected in the next scheduled Publication of Digital Certificate status information.

The DIP shall processes all CRRs within 24 hours, unless the circumstances of the case require otherwise.

## CRL issuance frequency

An up to date version of the DIP-PKI CRL shall be 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:

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

## On-line revocation/status checking

The validity interval of an Online Certificate Status Protocol (OCSP) response is the difference in time as noted by the DIP between one status being published and the next update. 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:

1. OCSP responses MUST have a validity interval greater than or equal to eight hours;
2. OCSP responses MUST have a validity interval less than or equal to ten days;
3. for OCSP responses with validity intervals less than sixteen hours, the DCA shall update the information provided via an OCSP prior to one-half of the validity period before the next update; and
4. for OCSP responses with validity intervals greater than or equal to sixteen hours, then the DCA shall update the information provided via an OCSP at least eight hours prior to the next update, and no later than four days after the last update.

For the status of subordinate DCA Certificates the DCA shall update information provided via an OCSP responder:

1. at least every twelve months; and
2. within 24 hours after revoking a subordinate DCA Certificate.

OCSP responders that receive a request for status of a Digital Certificate that has not been issued, shall not respond with a ‘good’ status for such Digital Certificates.

OCSP responders for DCAs which are not technically constrained shall not respond with a ‘good’ status for such Digital Certificates.

## Actions in the event of a Private Key compromise

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

1. immediately notify the DIP Manager; and
2. provide the DIP Manager with all of the information known to it in relation to the nature and circumstances in the event of a compromise or suspected compromise.

Where the compromise or suspected compromise relates to any Private Key:

1. ensure that the Private Key is no longer used; and
2. notify each of the DIP Users for any Digital Certificates issued using that Private Key.

## End of subscription

Each DIP-PKI certificate has a lifecycle of 398 days. At the end of this period the relevant DIP User Digital Certificates will expire. The DIP Manager shall notify the DIP User of such expiry as laid out elsewhere in this DIP-PKI Policy and wider DIP Rules.

## Key escrow and recovery statements and practices

This DIP-PKI Policy does not cover key escrow services as the DCA is not permitted to provide any key escrow services.

The DIP-PKI Recovery practices shall be documented in the DIP-PKI CPS.

# Facility, management, and operational controls

## Overview

The facilities, management and operational controls for the manufacture of certificates are managed through the DIP CM.

The DIP CM shall ensure that their 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.

## Physical Controls

The IA shall ensure that, where Digital Certificate manufacture or time-stamping operations are carried out, they:

1. satisfy at least the requirements specified by either ISO 27001 or ETSI TS 319 401 (or similar standard at the DIP Manager’s discretion) for CAs for production and control of Certificates;
2. will be manually or electronically monitored for unauthorised intrusion at all times;
3. apply controls such that unescorted access to DCAs or time-stamping servers is limited to authorised personnel and:
   1. ensure unauthorised personnel are properly escorted and supervised;
   2. ensure a site access log is maintained and inspected periodically;
4. ensure all removable media and paper containing sensitive plain text information is stored in secure containers.

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

The DIP 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 exist.

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 exist.

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.

The DIP 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.

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

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.

## Procedural controls

The DIP CM shall provide for the separation of distinct DIP-PKI personnel roles by named personnel, distinguishing between day-to-day operation of the DCA 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 DIP-PKI CPS and/or supporting documentation.

The RA shall ensure that all RA personnel are adequately trained and understand their responsibility for the identification and authentication of prospective DIP Users and related Digital Certificate management tasks. The RA’s arrangements for trusted roles are laid out elsewhere in the DIP Rules (which for the purposes of this DIP-PKI Policy shall be the ‘registration policy and procedures’).

The IA and RA may permit all roles and duties to be performed by one individual.

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

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

The DIP 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:

1. included in the access list for the site of the DIP User providing Trust Services;
2. included in the access list for physical access to the Trust Service provider systems;
3. given a credential for the performance of their Trust Service provider role; and
4. given an access on Trust Service provider systems.

Credentials issued to personnel in trusted roles must be:

1. managed so that their use can be detected and monitored;
2. managed so that their use is restricted to actions authorised for that role through applicable technical and procedural controls;
3. maintained under a prescribed and documented security policy.

The DIP CM, in its assignment of duties among personnel, shall maintain appropriate separation of duties so as not to compromise the security arrangements for the DIP CM and other critical processes.

The CM shall provide and maintain records of role allocation.

## Personnel controls

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

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

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

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

## Audit Logging Procedures

The DIP-PKI CM shall ensure that in the DIP CM operations, audit logs of all transactions relevant to Digital Certificate creation, Digital Certificate lifecycle management and the operation of trusted systems and services are maintained to provide an audit trail. The event types to be logged include:

1. Messages received from authorised sources requesting an action on the part of the DCA;
2. all actions taken in response to requests;
3. trusted system installation and any modifications;
4. receipt, servicing and shipping of hardware cryptographic modules;
5. creation and issuance of CRLs;
6. all error conditions and anomalies associated with the operation of trusted systems and services;
7. any known or suspected violations of physical security;
8. any known or suspected violations of network and/or trusted system security;
9. all DCA and trusted application start-up and shutdown;
10. all usage of the DCA signing key; and
11. all personnel/role changes for trusted roles.

## The IA shall ensure the RA shall record for audit purposes, at minimum, the event types listed below:

1. any log on/off attempts by RA operators;
2. all messages from authorised sources requesting an action of the RA and the subsequent actions taken by the RA in response to such requests;
3. all messages to the CA requesting an action of the CA and the subsequent action taken by the CA;
4. all physical accesses to RA systems (including components) and RA locations;
5. RA application start-up and shut down;
6. all use of any RA signing key(s);
7. any suspected or known violations of physical security;
8. any suspected or known violations of network and system security;
9. all checks made for the registration of RA staff; and
10. all personnel/role changes for trusted roles.

The DIP CM shall provide details of audit log processing in the records of role allocation in the DIP-PKI CPS and/or supporting documentation. Procedures must be approved by the IA or auditors acting on its behalf.

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

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

The DIP CM shall ensure audit logs and audit summaries are backed up or, if in manual form are 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.

## Record archiving

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

The IA shall ensure the RA retains information provided in support of Digital Certificate application and revocation requests.

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

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.

The process for archiving is not subject to this DIP-PKI Policy; similarly there is no stipulation on time-stamping records

Records of individual transactions may be released upon request by any of the DIP 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 IA are to be interrupted, suspended or terminated, the IA shall ensure the continued availability of the archive. All requests for access to such archived information shall be sent to the IA or to the entity identified by the Issuing Authority prior to terminating its service.

## Key changeover

A DIP User may only replace their Digital Certificate and key pair prior to the expiration of the keys, provided that the current Digital Certificate remains valid and has not been revoked or suspended. This key changeover may be initiated by one of the following:

1. the DIP User or DCP;
2. the RA; or
3. the IA.

Automated notification of an impending required key changeover is permitted.

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

Where a DIP Users Digital Certificate has been revoked as a result of suspected or actual non-compliance, the IA shall verify that the reasons.

## Compromise and disaster recovery

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

In the case of comprise of a DCA or DCA-keys, the IA shall, as a minimum:

1. immediately suspend all issued Digital Certificates affected by a compromise, failure or disaster; and
2. prevent any further Digital Certificate issuance from the affected DCA.

The DIP 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 CPS and/or supporting documentation. Plans must be approved by the Issuing Authority.

The business continuity plan for the CM 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 DIP-PKI Policy shall be maintained during any relocation/transition.

# Technical Security Controls

## Key pair generation and installation

IA 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.

The IA must approve any processes for Private Keys used in any IA and/or Trust Service that affects the outcome of Issued Certificates and Certificate Status Information services

DIP Users conducting such key generation shall provide details of the procedure in the CPS and/or supporting documentation.

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

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 CA shall use PKCS#10 or other equivalent standards compliant cryptographic mechanism or using a process specifically approved by the CM. Specific mechanisms must be approved by the IA.

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.

## Key sizes and parameters

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

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

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

## Key usage purposes (as per x.509 v3 key usage field)

Certificates issued under this DIP-PKI Policy may be used in applications and services as listed below:

1. TLS client and server authentication between DIP Users and the DIP; and
2. digital signing of messages between DIP Users and the DIP.

Where a Digital 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 this DIP-PKI Policy.

## Private Key protection and cryptographic module engineering 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 IA and/or RA 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.

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

The DIP-PKI CM may backup and archive Private Keys including CA keys. DIP Users are responsible for the Back-Up of their own keys.

Key backups shall, as 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 IA private signing key.

## Private Key transfer into or from a cryptographic module

If DIP 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 IA. Mechanisms to protect key material and any associated activation data from unauthorised access, modification and use shall be employed.

DIP Users conducting such key transfer shall provide detail of the procedure in the CPS and/or supporting documentation. Procedures must be approved by the IA.

## Method of activating Private Keys

DIP Users’ staff 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.

Private Key deactivation is not subject to this DIP-PKI Policy.

## 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 IA must approve the destruction of such keys.

## Other aspects of key pair management

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

1. DIP User Certificate up to 398 days;
2. DIP-PKI CM five years.

## Activation Data

All IA 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.

All IA 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 CPS and/or supporting documentation. Procedures must be approved by the IA.

## Computer security controls

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:

1. access control to trust services and PKI roles;
2. enforced separation of duties for PKI roles;
3. identification and authentication of PKI roles and associated identities;
4. use of cryptography for session communication and database security;
5. archival of DIP Service User history and audit data;
6. audit of security related events;
7. trusted path for identification of PKI roles and associated identities; and
8. recovery mechanisms for keys of PKI DIP Users providing trust services.

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

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

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

Any hardware security module or device holding CA Keys must comply with the requirements of this DIP-PKI Policy.

Where specific computer security rating requirements are specified in this DIP-PKI Policy, details of relevant components and how they satisfy the requirements must be provided in the CPS and/or supporting documentation.

## Life Cycle Technical 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:

1. the system developer shall have a quality system compliant with international standards; or
2. the system developer shall have a quality system available for inspection and approval by the IA.

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 IA.

## 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 CPS and/or supporting documentation which must be approved by the IA.

The DIP-PKI CM shall implement time recording for all Digital Certificates 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 CPS and/or supporting documentation which must be approved by the IA.

# Certificate, CRL, and OCSP Profiles

## Certificate Profile

Certificate Profiles are under the direct control of the DIP Manager. The DCA shall only issue Digital Certificates in accordance with the Certificate Profiles in DSD002 Annex 2 ‘Detailed Connection Requirements’.

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

All End Entity PKI software must correctly process the extensions identified in the IETF RFC 5280 CPS. The following are common Certificate Extensions:

1. the Basic Constraints Extension is set to ‘TRUE’ for CA-certificates only; its use is critical in specifying that it is a CA-certificate. DIP User and End Entity Digital Certificates have the value set to ‘FALSE’;
2. the ‘Certificate Policies extension’ is mandatory within the CPS and shall contain a policy identifier (OID) indicating the use of this DIP-PKI Policy. The ‘Certificate Policy Qualifier Info’ extension to the CPS shall be used to direct End-Entities to where this DIP-PKI Policy and other relevant information may be found; and
3. 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 IA can be obtained.

The use of all name forms shall be consistent with this DIP-PKI Policy. Name forms shall be approved by the IA.

## CRL Profile

Only CRLs conforming to X.509 version 2 and IETF RFC 5280 may be issued.

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

## OCSP Profile

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

Repositories shall detail the mechanisms for on line Digital Certificate Status Information provision in the DIP-PKI CP and/or supporting documentation which must be approved by the IA.

# Compliance Audit and other assessments

## Frequency or circumstances of assessment

The details for assessment are specified in contractual arrangements between the IA and the DIP-PKI CM and DSD003 ‘Assurance and Reporting’.

Assurance processes must be sufficient to demonstrate to the IA that the services comply with this DIP-PKI Policy and any supporting policy documents applicable to their services.

The DIP-PKI CM assessment shall be against prescribed criteria defined by the Policy Authority and shall be conducted not less than annually and in accordance with the DIP Assurance Strategy.

## Identity/qualifications of assessor

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

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

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

## Assessor's relationship to assessed entity

The acceptability of auditors is decided by the Policy Authority.

## Topics covered by assessment

Assurance processes shall ensure the CA providing Trust Services, i.e. the DIP-PKI CM, is operating in accordance with its DIP-PKI CPS, this DIP-PKI Policy and any declared assurance or approval schemes under which Trust Services are operated.

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

## Actions taken as a result of deficiency

For compliance audits of the DIP-PKI CM, where significant exceptions or deficiencies are identified, the IA will inform the Policy Authority and determine the action to be taken and a remedial action plan will be developed. The Policy Authority has overall responsibility to ensure implementation of the action plan.

If an immediate threat to the security or integrity of the DIP-PKI services is identified, a corrective action plan, which may include suspension or termination of non-compliant services, will be developed and approved by the Policy Authority and implemented by the IA, notwithstanding the requirements of DSD002 ‘DIP Connection and Operation’ in respect of suspensions and DIP Off-boarding. For lesser exceptions or deficiencies, the IA will determine the course of action to be taken.

## Communication of results

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

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