UK e-Science Certification Authority
2A (PATHFINDER)
Certification Practices Statement
Version 0.1
(OID)

04 Mar 2017

1 INTRODUCTION

1.1 Overview

This is the Certification Practices Statement (CPS) for UK e-Science CA 2A (UKCA2A). The CA is a MICS CA, but can issue short-lived credentials to Subscribers which cannot comply with the full revocation requirements of MICS.

The Certificate Policy (CP) of UKCA2A is the CP for the UK e-Science CA, currently version 2.0 (1.3.6.1.4.1.11439.1.1.1.1.2.2.0).

Initially set up by GridPP as a contribution to the AAAI Pathfinder project, services are available to Subscribers at institutes with suitable IdPs in the JISC Assent project. The lifetime of UKCA2A is not limited to the duration of the Pathfinder project; the intention is that the CA be run alongside the Assent project.

1.2 Document name and identification

This document is the CPS of UK e-Science CA 2A

1.3.6.1.4.1.11439.1.1.1.1.2.2.0

1.3 PKI participants

The community of UKCA2A is in general terms the academic and research communities in the UK making use of national and international e-infrastructures and/or collaborating with similar researchers internationally.

1.3.1 Certification authorities

CA certificates for UKCA2A are issued by the UK e-Science Root.

1.3.2 Registration authorities

As UKCA2A is a MICS CA, there are no RAs as such; rather, the rôle of RA is fulfilled by authorised staff at the research institutions participating in Assent and qualifying for inclusion in the CoI.

An IdP can be joined into the COI only if every identity it asserts to the CA (as an Assent service provider) complies with the BIRCH requirements (see 3.2. The organisation running the IdP takes full legal responsibility for the correctness of assertions issued by the IdP, and promises to notify the CA immediately if the status changes.

1.3.3 Subscribers

UKCA2A issues only personal certificates. These are issued to members of the organisations participating in Assent. Certificates can be requested only for their personal use. In particular, End Entities (as defined in the CP) are always the same entity as the Subscriber.

1.3.4 Relying parties

There are two types of RPs for UKCA2A, national and international. National research infrastructures that are directly reliant on the CA through their participation in AAAI Pathfinder are GridPP (www.gridpp.ac.uk), eMedLab (www.emedlab.ac.uk), Oxford's Advanced Research Computing, ARCHER (www.archer.ac.uk), DiRAC (www.dirac.ac.uk).

Secondly, recognised RPs are those represented by the PMAs, whether represented directly by a named person or indirectly via a national CA.

1.3.5 Other participants

JISC (www.jisc.ac.uk), through its leadership of Assent, is a participant. Also the project management of AAAI Pathfinder is a participant, for the duration of the Pathfinder project.

1.4 Certificate usage

Only personal certificates are issued; the main supported purpose is user authentication.

1.4.1 Appropriate certificate uses

Use of certificates is subject to the JISC Network AUP.

Subscribers may use their certificates to:

- Create proxy certificates
  - Proxy certificates are also subject to the CP and this CPS
- Authenticate to services
- Send signed email
- Or make other digital signatures
- Upload private key and certificate to a key repository, provided it complies with the requirements of IGTF.

Participants may use certificates to:

- Verify digital signatures
- Encrypt email to a recipient
- Extract keys for similar use

1.4.2 Prohibited certificate uses

Using certificates for purposes that violate the JISC Network AUP is prohibited.

At no time may a private key be used by someone other than the Subscriber if a certificate is issued, or is to be issued, by this CA containing the corresponding public key, with one exception:

Anyone other than the Subscriber with access to the activated private key should request revocation of the certificate. Revocation should be requested irrespective of the lifetime of the certificate.

1.5 Policy administration

This document is subject to the CP of the UK e-Science CA. It is modified in consultation with the principal stakeholders, namely the national RPs described in 1.3.4, and JISC.

1.5.1 Organization administering the document

This document is managed by STFC on behalf of GridPP.

1.5.2 Contact person

Questions or comments should be sent to the support helpdesk; see www.ngs.ac.uk.

1.5.3 Person determining CPS suitability for the policy

Suitability is determined by the UK e-Science CA.

1.5.4 CPS approval procedures

The CPS needs approval by:

- Internal process
- EUGridPMA (www.eugridpma.org)

1.6 Definitions and acronyms

See 1.6 of the CP.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

The CA repository can be found at http://www.ngs.ac.uk/.

2.1 Repositories

An online, web-accessible interface shall be run which permits the user to:

- Unauthenticated
  - Locate support and information, including CP and CPS
  - Locate and download the CRL
- Authenticated, using any Assent IdP
  - Test attribute release and view eligibility status
- Authenticated, using an IdP which is part of the required COI
  - Request a new certificate, or rekey or revocation of an existing certificate

2.2 Publication of certification information

No stipulation.

2.3 Time or frequency of publication

All public information is made available aiming for a 24/7 availability subject to scheduled network and service interventions.

2.4 Access controls on repositories

Following the policy, there are no access controls on public information repositories; interfaces accessible to individual users require Assent authentication as described in 2.1.

3 IDENTIFICATION AND AUTHENTICATION (11)

3.1 Naming

Naming shall follow GFD.225 and RFC 5280.

3.1.1 Types of names

Subject Distinguished and Alternative Names are X.500 DNs and RFC 822 (email), respectively.

3.1.2 Need for names to be meaningful

DNs issued to Subscribers shall contain

- the name of their organisation, and
- a reasonable representation of the user's authenticated name (i.e. rendered compliant with GFD.225).

3.1.3 Anonymity or pseudonymity of subscribers

Names are neither anonymous nor pseudonymous; it is the responsibility of the IdPs to publish the Subscriber's name (any standard given name/surname combination) and to ensure it is accurate; it is the responsibility of the CA to ensure the name is mapped to a form compliant with GFD.225.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

DNs are uniquely associated to each individual through their organisational affiliation. Users who change their organisational affiliation will, in general, change their DN. See 7.1.4.

Uniqueness should not be assumed based on the CN alone. See *ibidem*.

Uniqueness is ensured through unique identifiers published by the IdP. IdPs have asserted that they comply with the uniqueness requirement.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

By being joined into the COI, IdPs assert that they have validated the identity of the Subscriber at a level sufficient to comply with BIRCH, and that they continue to comply with this for as long as any certificate issued through the IdP remains valid.

We list the requirements here, but the reader should note that the authoritative source is the IGTF AP version 1.0, and in case of any discrepancy or difference in interpretation between this document and the IGTF AP, the latter takes precedence. However, when we here pick a subset of the BIRCH profile, the intention is to narrow and specialise the requirements to this subset.

Specifically, the organisation running the IdP promises to:

- (AP3.1) **Uniqueness.** Publish sufficient information to the CA to enable the CA to uniquely identify any authenticating user; this attribute should be persistent, i.e., the same every time the same user authenticates to the CA.
- (AP3.1) **Traceability** Retain sufficient records to link the identifying attributes to the user's real-life identity, throughout the lifetime of the certificate (see XXX)
- (AP4.3) Upon loss of this Traceability, the IdP shall
  - Revoke the individual's ability to authenticate through the IdP, and
  - If it can, notify the CA so the certificate can be revoked.
  - If the IdP lacks the ability or permission to notify the CA, the CA shall issue only SLCs for this IdP.
- (AP3.1) Users authenticated by the IdP must have shown reliable photo id and/or valid official identity documents *in person* to a trusted agent of the organisation.
- (AP5) **Incident resolution.** Cooperate with the CA and/or JISC in the case of an incident.

In addition, it is recommended that IdPs comply with SIRTFI.

3.2.1 Method to prove possession of private key

Private keys are generated either by users themselves or directly on their behalf and instigation in the credential store, upon requesting a certificate.

3.2.2 Authentication of organization identity

It is the responsibility of the IdP to publish to the CA a string representing the corporate identity of the organisation. Organisations should be legal entities which are members of Assent.

3.2.3 Authentication of individual identity

Individuals authenticate to the CA and to the credential store using Assent.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

No stipulation.

3.2.6 Criteria for interoperation

Certificates issued by the CA shall comply with GFD.225.

3.3 Identification and authentication for re-key requests

As authentication for the initial request.

3.3.1 Identification and authentication for routine re-key

As authentication for the initial request.

3.3.2 Identification and authentication for re-key after revocation

As authentication for the initial request.

3.4 Identification and authentication for revocation request

As authentication for the initial request, using Assent; or alternatively upon authenticating with the certificate (using the associated private key).

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS (11)

4.1 Certificate Application

Applications are made using a web browser to the CA's access controlled repository.

4.1.1 Who can submit a certificate application

Any member who can authenticate with an IdP compliant with the BIRCH requirements, run by an organisation that is member of Assent.

4.1.2 Enrollment process and responsibilities

No stipulation.

4.2 Certificate application processing

Once made, a request is automatically approved and will be signed by the CA at the earliest opportunity.

4.2.1 Performing identification and authentication functions

It is the responsibility of the organisation running the IdPs to perform Subscriber authentication and identity verification and the retention of the audit logs according to the BIRCH requirements, see 3.2.

4.2.2 Approval or rejection of certificate applications

A user authenticating with an Assent IdP that does is not a member of the COI will have their certificate request rejected.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

A certificate is issued directly to the user, or, when applicable, to the credential store.

4.3.1 CA actions during certificate issuance

No stipulation.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Subscriber is notified through the web interface or via email.

4.4 Certificate acceptance

No stipulation.

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

Certificates are not published by the CA.

4.4.3 Notification of certificate issuance by the CA to other entities

Notification of issuance is given, when applicable, to the approved credential store(s) linked to the CA.

4.5 Key pair and certificate usage

The CA certificate and private key are used to verify and sign end entity certificate, as well as signing CRLs.

4.5.1 Subscriber private key and certificate usage

Generation and use of the private key must follow the IGTF private key protection guidelines. In particular, the Subscriber is at all times responsible for the correct management – including protection – of their private key.

4.5.2 Relying party public key and certificate usage

Relying Parties use the CA certificate to verify the signature of end entity certificates and of the CRLs.

4.6 Certificate renewal

Certificate renewal is not supported.

4.6.1 Circumstance for certificate renewal

Certificate renewal is not supported.

4.6.2 Who may request renewal

Certificate renewal is not supported.

4.6.3 Processing certificate renewal requests

Certificate renewal is not supported.

4.6.4 Notification of new certificate issuance to subscriber

Certificate renewal is not supported.

4.6.5 Conduct constituting acceptance of a renewal certificate

Certificate renewal is not supported.

4.6.6 Publication of the renewal certificate by the CA

Certificate renewal is not supported.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Certificates may be routinely rekeyed either prior to the expiry of the certificate, or upon changing information held in the certificate. In the latter case, the earlier certificate shall be revoked if it is long lived.

4.7.2 Who may request certification of a new public key

Only the Subscriber or the authorised credential management service(s) may request certification of a new public key.

4.7.3 Processing certificate re-keying requests

Rekey requests are processed like a new request, including the validation of the identity. However, a long-lived certificate is being rekeyed, whose expiry is further than 30 days in the future, the CA may do any or all of the following:

- Refuse the renewal;
- Revoke the current certificate upon issuance of the new one, or a set number of working days after the issuance of the new certificate;
- Require approval by an authorised person.

4.7.4 Notification of new certificate issuance to subscriber

As new requests.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As new requests.

4.7.6 Publication of the re-keyed certificate by the CA

As new requests.

4.7.7 Notification of certificate issuance by the CA to other entities

As new requests.

4.8 Certificate modification

Certificate modification is done through rekey.

4.8.1 Circumstance for certificate modification

Certificates must be modified in the following cases:

- The user's name changes (as published by the IdP);
- The user's email address, as embedded in the Alternative Name, ceases to be valid;
- The user's organisational affiliation – or organisation's name – changes;

4.8.2 Who may request certificate modification

Certificates may be modified upon Subscriber request.

4.8.3 Processing certificate modification requests

If the certificate modification is based entirely on information published by the IdP, the modification is accepted directly. If the modification requires additional attributes, particularly those conferring additional privileges, an approval by an authorised agent may be required.

4.8.4 Notification of new certificate issuance to subscriber

As new requests.

4.8.5 Conduct constituting acceptance of modified certificate

As new requests.

4.8.6 Publication of the modified certificate by the CA

As new requests.

4.8.7 Notification of certificate issuance by the CA to other entities

As new requests.

4.9 Certificate revocation and suspension

All EE certificates can be revoked. Expired certificates may be removed from the CRL.

4.9.1 Circumstances for revocation

As per the policy.

4.9.2 Who can request revocation

As per the policy. Note that only authenticated entities can request revocation.

4.9.3 Procedure for revocation request

The CA runs an interface for revocation requests.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

Approval or rejection of the CRR is done instantly (algorithmically) by the CA.

4.9.6 Revocation checking requirement for relying parties

As per the policy.

4.9.7 CRL issuance frequency (if applicable)

CRLs are issued and published at each revocation, and at least daily.

4.9.8 Maximum latency for CRLs (if applicable)

The most recently signed CRL shall be made available online according to repository obligations, 2.1.

4.9.9 On-line revocation/status checking availability

OCSP is not currently supported.

4.9.10 On-line revocation checking requirements

As per the policy.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

No stipulation.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

No stipulation.

4.10.1 Operational characteristics

Secure services are available for all sensitive information and privileged actions. Authentication will be required for access to non-public information.

4.10.2 Service availability

The CA aims to make its online services available 27/7 subject to scheduled maintenance. The data centre operates a network-at-risk period on Tuesday mornings where short interventions may be made without warning (e.g. reboot for patches, etc.).

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

No stipulation.

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

The data centre that hosts the physical infrastructure of the CA is access controlled, with CCTV monitoring and access limited to authorised personnel.

5.1.1 Site location and construction

The data centre is

5.1.2 Physical access

Site access is monitored by on-site security which are available 24/7 throughout the year and are physically located immeditaly next to the building hosting the data centre. Physical access to the building requires an authorised key outside of office hours; physical access to the data centre within the building requires an authorised key at all times.

Furthermore, physical access to the CA infrastructure within the data centre requires an additional key, as the hardware is locked in a cage within the data centre.

5.1.3 Power and air conditioning

The data centre has a backup generator which is tested at least every six months. The generator is capable of running essential services for at least 24 hours without refuelling. Moreover, UPS services are also available in the

data centre; however, currently only networks and not the CA hardware is on UPS.

5.1.4 Water exposures

There are no water carrying pipes above or in the immediate neighbourhood of the CA hardware.

5.1.5 Fire prevention and protection

The data centre has fire suppression/protection (fire retardant gas released), and smoke and fire detection sensors.

5.1.6 Media storage

No stipulation.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

No stipulation.

5.2.1 Trusted roles

No stipulation.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

Authentication to and activation of the HSM is done through role-based token with PIN activation.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

No stipulation.

5.3.1 Qualifications, experience, and clearance requirements

No stipulation.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Unauthorised activities are sanctioned through STFC's normal IT policy and disciplinary processes.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No stipulation.

5.4 Audit logging procedures

No stipulation.

5.4.1 Types of events recorded

The CA logs all certificate requests and issuances, as well as the associated metadata such as originator IP and organisation, session id, timestamp.

5.4.2 Frequency of processing log

No stipulation.

5.4.3 Retention period for audit log

Service logs are retained for at least three months; logs pertaining to the issuance of certificates are maintained for at least the lifetime of the certificate and up to two years after the expiry of the certificate.

5.4.4 Protection of audit log

Best practices are employed to ensure that logs are irreversible and tamper proof.

5.4.5 Audit log backup procedures

No stipulation.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

No stipulation.

5.5 Records archival

No stipulation.

5.5.1 Types of records archived

No stipulation.

5.5.2 Retention period for archive

No stipulation.

5.5.3 Protection of archive

No stipulation.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

Timestamping accuracy is achieved through synchronisation with the NTP services.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

Changeover of CA certificates follows IGTF best practices.

5.7 Compromise and disaster recovery

No stipulation.

5.7.1 Incident and compromise handling procedures

As a SIRTFI site, STFC must contribute to the satisfactory resolution of incidents, and must thus require the appropriate contributions from the relevant organisations running IdPs.

5.7.2 Computing resources, software, and/or data are corrupted

No stipulation.

5.7.3 Entity private key compromise procedures

No stipulation.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA termination

In case of termination of the CA, it shall be withdrawn from the IGTF distribution and announcements are made through the IGTF notification list.

6 TECHNICAL SECURITY CONTROLS (11)

6.1 Key pair generation and installation

As of this version of the CPS, the CA's private key is generated inside the HSM; in particular, while the encrypted key is backed up, it has no backup independent of its host HSM, nor is it backed up in any of the other HSMs.

It is the intention that the CA be rekeyed towards the end of 2017, with improved DR; this activity is expected to be part of a larger activity to move other CA certificates to SHA2 signatures.

6.1.1 Key pair generation

EE key generation follows IGTF PKP guidelines.

6.1.2 Private key delivery to subscriber

Not applicable; Subscribers either generate their own private key, or it is held only in the credential store.

6.1.3 Public key delivery to certificate issuer

The certificate is delivered to the user via the portal or to the credential store.

6.1.4 CA public key delivery to relying parties

The CA public key is made available – through the CA certificate, signed by the root – via the CA's repository/repositories, and through the IGTF distribution.

6.1.5 Key sizes

The CA follows IGTF best practices for key sizes.

6.1.6 Public key parameters generation and quality checking

No stipulation.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Certificates (CA and EE) will have the minimal required extensions to support their purposes, as described in GFD.225.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The CA's private key is stored in a HSM which has been certified to FIPS-140-2 Level 3 (operating at Level 3).

6.2.2 Private key (n out of m) multi-person control

There is no n-of-m for $n > 1$.

6.2.3 Private key escrow

No private keys are escrowed.

6.2.4 Private key backup

Currently the key is only installed on a single HSM (see 6.1) and is backed up only as a part of that particular HSM.

6.2.5 Private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

The key was generated inside the HSM.

6.2.7 Private key storage on cryptographic module

The private key is encrypted by the HSM and stored only in encrypted form.

6.2.8 Method of activating private key

As the CA is an online CA, the private key remains active essentially at all times; however a system reboot normally requires reactivation of the key.

6.2.9 Method of deactivating private key

The key can be deactivated physically by removing a smart key, or remotely by stopping a daemon.

6.2.10 Method of destroying private key

No stipulation.

6.2.11 Cryptographic Module Rating

The HSM is certified to FIPS-140-2 Level 3.

6.3 Other aspects of key pair management

No stipulation.

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

No stipulation.

6.4 Activation data

No stipulation.

6.4.1 Activation data generation and installation

The best practices as recommended by the HSM vendor are followed.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

The HSMs and the computers accessing and monitoring them are located in a data centre with physical security, including the building, 24/7 CCTV monitoring, 24/7 security on site, and access control to the machine room. In addition, the computers are hosted in a rack in a locked cage inside the machine room.

6.5.1 Specific computer security technical requirements

Signing system must be (and is) dedicated (doing only signing) and other CA-related tasks; and the HSMs are certified to FIPS140-2, operating at Level 3.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

No stipulation.

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

Site procedures for operating and decommissioning sensitive systems are followed.

6.7 Network security controls

Access to HSMs is over dedicated physical links.

6.8 Time-stamping

Time is synchronised against internal NTP servers.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificate profile follows GFD.225.

7.1.1 Version number(s)

Certificates are version 3.

7.1.2 Certificate extensions

Extensions are allocated to certificates following GFD.225 profile for user certificates.

In particular, the user's email address, as published by the IdP, is embedded in the certificate.

7.1.3 Algorithm object identifiers

The IGTF recommended signature algorithm is used.

7.1.4 Name forms

Names are X.500 names, structured according to GFD.225 recommendations. The distinguished names are:

`/DC=uk/DC=ac/DC=pathfinder/O=`*org*`/CN=`*name num*

where *org* is the organisation name as published by the IdP, and *name* is the GFD.225-compliant representation of the user's common name as published

by the IdP. In addition, *num* is a five digit number which is included to ensure uniqueness (see section 3.1.5.)

7.1.5 Name constraints

The name constraints extension (in the CA certificate) is *not* used.

The CA will issue RPDNC namespace constraints as well as Globus signing policy files, covering its issued certificates.

The name part `/DC=uk/DC=ac/DC=pathfinder` is fixed for all end entities.

7.1.6 Certificate policy object identifier

The OID of the CP is `1.3.6.1.4.1.11439.1.1.1.2.2.0`.

The following OIDs will be asserted in the certificatePolicies extension (and in the following order):

- The OID of the CP.
- `1.2.840.113612.5.2.2.5` – MICS (BIRCH X.509 C)A
- `1.2.840.113612.5.2.3.3.3.1` – entity is a natural person

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

Critical certificate extensions must be processed according to RFC 5280, section 4.2.

7.2 CRL profile

CRLs are structured according to RFC 5280.

7.2.1 Version number(s)

CRLs will be version 2.

7.2.2 CRL and CRL entry extensions

CRLs may have extensions and/or entry extensions; in which case these extensions follow RFC 5280.

7.3 OCSP profile

No stipulation.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

See the CP.

8.1 Frequency or circumstances of assessment

See the CP.

8.2 Identity/qualifications of assessor

See the CP.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

See the CP.

8.5 Actions taken as a result of deficiency

See the CP.

8.6 Communication of results

See the CP.

9 OTHER BUSINESS AND LEGAL MATTERS

See the CP.

9.1 Fees

See the CP.

9.1.1 Certificate issuance or renewal fees

See the CP.

9.1.2 Certificate access fees

See the CP.

9.1.3 Revocation or status information access fees

See the CP.

9.1.4 Fees for other services

See the CP.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

See the CP.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

No stipulation.

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

See the CP.

9.4 Privacy of personal information

See the CP.

9.4.1 Privacy plan

See the CP.

9.4.2 Information treated as private

See the CP.

9.4.3 Information not deemed private

See the CP.

9.4.4 Responsibility to protect private information

See the CP.

9.4.5 Notice and consent to use private information

See the CP.

9.4.6 Disclosure pursuant to judicial or administrative process

See the CP.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

See the CP.

9.6 Representations and warranties

No stipulation.

9.6.1 CA representations and warranties

See the CP.

9.6.2 RA representations and warranties

The process that joins an IdP to provide identity to this CA is manual. A person representative of the organisation running the IdP, who is authorised and qualified to make such assertions, shall assert compliance with the IdP BIRCH requrements (section 3.2).

To be clear, it is the organisation that runs the IdP that must make the assertion, and is held responsible for the operation and compliance of the IdP, as defined in the Assent

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

See CP.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

See CP.

9.10.2 Termination

See CP.

9.10.3 Effect of termination and survival

No stipulation..

9.11 Individual notices and communications with participants

Communication is made through the PMAs, through IGTF, or through Assent, as appropriate.

9.12 Amendments

See CP.

9.12.1 Procedure for amendment

See CP.

9.12.2 Notification mechanism and period

See CP.

9.12.3 Circumstances under which OID must be changed

See CP.

9.13 Dispute resolution provisions

See CP.

9.14 Governing law

See CP.

9.15 Compliance with applicable law

See CP.

9.16 Miscellaneous provisions

See CP.

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

See CP.

9.16.3 Severability

See CP.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

See CP.

9.17 Other provisions

See CP.