UK e-Science Certification Authority Certificate Policy Version 2.0 (20150304) 1.3.6.1.4.1.11439.1.1.1.2.2.0

Scientific Computing Department

Science and Technology Facilities Council

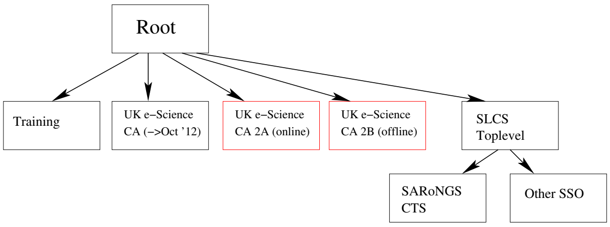
05 Aug 2010 – 23 Jun 2014

1 INTRODUCTION

This document describes the Certificate Policy for UK e-Science. The document defines policies for all authorities and all credentials issued by these authorities.

1.1 Overview

The UK e-Science PKI is structured as follows:



The diagram shows a Root CA with an IGTF-accredited CA underneath it, with two current certificates (highlighted in red if you have a colour document). The hierarchy also contains an older certificate for the same CA, as well as a toplevel CA which itself signs SLCS CAs.

The hierarchy contains CAs with different Levels of Assurance (LoAs). These LoAs are defined in this document, with the general overview in this section.

In describing the LoAs in this document, the following aspects are considered:

- Protection of the CA's Secret;
- Assurance associated with validation of Certificate Assertions at the time of approval of the Certificate Signing Request;
- Protection of Subject's Secret;
- Timeliness of Certificate Assertions.

The following table gives an outline of the role of the LoAs in the hierarchy.

LoA	**KeyProt**	**Subj.Val.**	**Subj.Key**	**Time**	**IGTF**
LoA0	Offline/manual	Offline/manual	CA keys only	Annual CRL	HLCA
LoA1	Offline/manual	HSM L3	IGTF	Working day	Classic
LoA2	Online/auto	HSM L3	IGTF	No revoc.	SLCS
LoA3	Online/auto	HSM L2	IGTF	No revoc.	IOTA
LoA4	Online/auto	Software	-	No revoc.	-

It should not be assumed that a higher level CA can fulfil the role of one at a lower level.

1.2 Document name and identification

Document identifier	UK-NGI-CA-Authority-CP
Version	2.0
OID	1.3.6.1.4.1.11439.1.1.1.1.2.2.0

{`iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) stfc(11439)`[1] `site-independent(1) escience(1) ca(1) cp(2) version(2) minor-version(0)`}.

1.3 PKI participants

The reader is warned that some of these definitions may be different from those found in RFC3647.

1.3.1 Certification authorities

- Issuing Authority (IA). We define an Issuing Authority as the component of a CA which issues certificates.

1.3.2 Registration authorities

- Registration Authorities (RA). Participants who are registered with a CA, who validate information contained in Requests submitted to the CA, and either approve or reject the request accordingly.
- Sponsors. In certain cases, the issuance of a certificate of a certain type to a Subscriber on behalf of a given EE may have to be sanctioned by a third party. This third party is referred to as the Sponsor of the certificate. It is the responsibility of the CA to ensure that this validation is performed and recorded in auditable form.

1.3.3 Subscribers

- Subscribers. Natural persons who interact with one or more CAs to request certificates, to whom certificates are issued, and who are responsible for the certificates and the corresponding private keys for as long as the private key exists in unencrypted or otherwise activated form.
- Credential – defined as the certificates, along with their associated Secrets, that are issued to a single End Entity based on an initial CSR, and subsequently renewed, rekeyed, or modified, from time to time. Typically all certificates associated with a Credential have the same DN, unless the DN is modified.

[1] Formerly known as CCLRC; STFC re-registered the OID when the organisation changed its name.

- End Entity (EE). The entity named as the Subject of a certificate. Entities who or which Use certificates for their Permitted Purposes, who are named in the certificate Subject DN and/or subject alternative names according to rules specified in the applicable policies.

  In this document, we shall refer to the Subscriber to whom a certificate is issued as the "owner of the certificate."

  If the EE is a natural person, we shall refer to the certificate as a *personal certificate.*

  In this document, we shall refer to "the EE's certificate" when the EE:

  1. is in possession of the certificate; and
  2. is named in the certificate Subject DN and/or subject alternative name; and
  3. is in possession of the Usable Private Key corresponding to the certificate; and
  4. is authorised by the Subscriber who requested the certificate to Use it.

  If the EE possesses more than one such certificate, the term may refer to any of them. Conversely, the EE named in the certificate shall be referred to as "the certificate's Subject."

1.3.4 Relying parties

- Relying Parties (RP). Participants who receive and validate certificates for any Permitted Purpose, who validate these certificates and any associated assertions according to rules set out in the applicable policies, and who Use certificates for the intended purpose only.

1.3.5 Other participants

- The *Technical Advisory Group* (TAG) consists of technical experts representihg major RPs, and is chaired by the manager of the UK e-Science CA.

1.4 Certificate usage

The Use of any certificate for its supported purposes must be supported, and to the extent reasonably possible, guaranteed, by the CA throughout the lifetime of the CA. CAs must not hinder the Use of certificates for their unsupported purposes.

CA certificates are issued for CA operations: certificate signing and CRL signing. CA certificates must not be Used for any other purpose.

Certificates must not be Used for commercial purposes.

1.4.1 Appropriate certificate uses

Each CA must define the permitted purposes of the certificates it issues. A CA must support the appropriate Uses of certificates that it issues as long as the support is needed.

A CA certificate must be used only for the validation of certificates that it has issued, including checking signatures of the certificate and checking (if applicable) CRL signatures.

IGTF EE certificates can always

1.4.2 Prohibited certificate uses

A CA must define Prohibited Uses of its certificate. A CA certificate must not be used for any purpose not defined in section 1.4.1 — in other words, any purpose which is not Permitted is Prohibited.

EE certificiates may have Uses which are neither appropriate (i.e. Supported) nor Prohibited. Such Use of the certificates need not be supported by the CA.

Notwithstanding the above, Using any certificate for financial transactions is prohibitied.

1.5 Policy administration

1.5.1 Organization administering the document

This document is administrated by the Science and Technology Facilities Council, STFC - `http://www.stfc.ac.uk/`.

1.5.2 Contact person

The person responsible for this document is:

Dr Jens Jensen
Science and Technology Facilities Council
Harwell Oxford Campus
Oxon, OX11 0QX
UK

1.5.3 Person determining CPS suitability for the policy

For a CA operating under the policy described in this document, it shall be the responsibility of the CA manager to ensure that the CPS is suitable for the policy and that any necessary review procedure is completed.

1.5.4 CPS approval procedures

A CA seeking IGTF accreditation must have a CPS and must structure it according to RFC 3647. The approval procedure in this case should involve the reviewers appointed by the IGTF.

For CAs not seeking accreditation with the IGTF, CAs of LoAs 0-2 should have a written and published CPS, published in a CA repository. They need not use RFC 3647. They should ensure that the compliance with this policy is checked by someone other than the author.

1.6 Definitions and acronyms

The following terms are defined in RFC 3647, to which the reader is referred ([?]).

Certificate Assertions – assertions about the Subject contained in the certificate, as well as implicit assertions associated with the certificate issuance and/or the possession of the certificate.

Certificate Request – a Request which, when approved, will cause the IA to issue a certificate to the Subscriber. Certificate Requests are typically CSRs or CCRs (see "Request" below.)

Compromise – of a Secret, the unauthorised exposure of all or parts of the Secret to a party not authorised to Process the key; including an otherwise authorised party gaining access to the Secret beyond that to which they are authorised. Specifically, of a private key, exposed in active form (or a form which can be activated with moderate effort), to an entity who is not the Subscriber, or, End Entity, or otherwise designated as being authorised to Process they key. Of a certificate, Compromise of the private key associated to the certificate.

Invalid – of a certificate, not Valid.

Lifetime – of a certificate, the interval of time after the notBefore time encoded in the certificate, and before the notAfter time. Also, occasionally, used to denote the length (in time) of this time interval.

Named – of a certificate, where the subject DN contains a reasonable representation of the name of the End Entity represented by the certificate, and where this representation has been verified by the CA and recorded in auditable form. In particular, a Named certificate is neither pseudonymous nor anonymous.

Names – of a Request or certificate, the Subject Distinguished Name and subject alternative names.

Personal – of certificates, where the End Entity is a natural person, and is named as the Subject of the certificate.

Process – of Information, to inspect, record, store, and use according to Applicable Law and the applicable policies.

Rely – a Relying Party is said to Rely on a certificate if they accept it at a specific time for a particular purpose.

Reliance – the state of Relying on something.

Request – means a certificate signing request (CSR), a certificate revocation request (CRR), a certificate change request (CCR), or any other request similarly associated with the issuance of, change of, or change of Validity of, a certificate. For the purposes of this document, a CSR is always signed with the private key corresponding to the public key in the request. The phrase "certificate request" is used for requests which are not necessarily signed.

Short Lived – of certificate, having lifetime less than one million seconds.

Subject – the entity who, or which, will be represented with a certificate.

Uniqueness – the quality of a Credential issued to a single Named Subject, that the Names are provably associated with only the Subject to which it is originally issued.

Valid – at a given time, a certificate is Valid if the given time is within the Lifetime of the certificate, and the certificate has not been suspended or revoked at that time. If a time is not stated explicitly, the intention is that the current time is used, e.g. at the time of Reliance.

Validity – of a certificate at a given time, the quality of being Valid.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

A CA conforming to this policy must operate an online repository, unless it conforms to LoA 3-4 *and* does not seek IGTF accreditation. If required to operate a repository, the following information must be published:

- The Trust Anchor(s) of the CA;
- Supplementary certificate status information, if certificate status other than those derived from the certificate itself are supported. In this case, such information shall be sufficient to determine the full status of the certificate at the current time;
- If any Permitted Purpose of the certificate may require determining the status of the certificate at a time other than the current time, such additional information shall also be published;
- Its policy and CPSes.

Best efforts should be made to ensure that repositories are available continuously subject only to essential scheduled maintenance.

2.2 Publication of certification information

Each CA should define how much, if any, of its issued certificates are public.

2.3 Time or frequency of publication

All public information must be published in a timely fashion. For revocation associated with the compromise of a private key, the CA should make every effort to ensure that the revocation information is published as soon as possible after the need for revocation has been established.

2.4 Access controls on repositories

All public information must be made available with no access control.

Information which is Processed by a CA but is not public must be protected.

3 IDENTIFICATION AND AUTHENTICATION

- All Subscribers and RA Operators must have Valid Personal Medium Assurance certificates. These certificates must be used to authenticate to the CAs.
- Identification of EEs XXX

3.1 Naming

Subject Names are X.500 Distinguished Names, or subject alternative names extensions, or both.

Before requesting a certificate, it is the responsibility of the Subscriber to ensure

1. That all names submitted in the CSR are owned by or allocated to the End Entity that will Use the certificate; and,
2. That all such names are sufficiently accurately represented in the DN and subject alternative names submitted in the CSR; and
3. All names contained in the CSR must be associated with the same EE; and
4. All Information necessary and sufficient to validate the association between the EE and the names presented in the CSR to the extent required by the applicable policies is made available to the appropriate RA Operator; and
5. The RA Operator is granted permission to Process such Information as required by the applicable policies; and
6. In the case of pseudonymous names, the link between the real identity of the EE and that of the pseudonym is recorded and maintained, and remains available for auditing and traceability purposes, throughout the Lifetime of the certificate.

It is also the responsibility of the Subscriber to ensure that

- The certificate can be Used by only by its EE; and
- It is allocated only to a single EE throughout the Lifetime of the certificate; and,
- For CAs that guarantee Uniqueness, that the certificate is allocated only to a single EE throughout the lifetime of the CA.

It is the responsibility of the CA to ensure that

- Any given DN is issued to a single Subscriber during the lifetime of the certificate;
- For CAs that offer Uniqueness, that any given DN is issued to a single Subscriber.

Specific rules regarding assignment and interpretation of Names are as follows:

DN – (1) The DN shall be interpretable as a string, *i.e.* in its textual representation: while it is permitted to use the DN in its encoded form, a CA shall not issue certificates which rely solely on the encoded form for the correct interpretation of the DN. (2) RPs should not rely on parts of the DN for authorisation.

Email – Email addresses used in certificates are expected to be valid in the sense that email sent to the address will be received by the Subscriber. It is not required that the Subscriber can send mail from the address.

DNS – a DNS name identifying a host (physical or virtual) should use the . The DNS name need not resolve, but should be in a DNS namespace controlled by the Subscriber, as per (3.1). Multiple DNS names may be present if they are associated with the same End Entity.

IP – IP addresses in certificates may be used. If so, they shall be statically allocated to a single host (physical or virtual).

3.1.1 Types of names

Names are Distinguished Names. Other name forms may be used in addition to distinguished names. Unless specified otherwise, names must be encoded as printableString, and a CN attribute must be used for a name RDN which contains the representation of the Subject's name. Other CNs may be present. The CN which contains the Subject's name can contain other information, but it is recommended that it be clear which parts are the Subject's name and which are not.

3.1.2 Need for names to be meaningful

Unless the CA explicitly allows anonymity or pseudonymous certificates, for personal credentials where the Subscriber is the Subject, the DN must contain a reasonable representation of the Subject's verified name.

For host certificates, the CN must either be

- A syntactically valid DNS name (the validity check that used to be RFC 1034), but need not actually resolve in DNS.
- A wildcard DNS name. In this case, the wildcard uses a '*' character and must be the first component of the name, or a part of the first component of the name.

3.1.3 Anonymity or pseudonymity of subscribers

Credentials can be pseudonymous.

Credentials which are not pseudonymous must, by definition, contain the proper name of the EE which is to be identified by the credential.

Pseudonymous credentials must be used only for personal credentials. It is the responsibility of the issuing authority to ensure that

- A mapping is retained between the verified name of the EE and the name presented in the credential (but it is not necessarily the responsibility of the authority to keep the data, only to ensure that it is kept.)
- This mapping is retained not only during the full lifetime of the credential, but also for a period of not less than six months beyond the expiry of the credential.
- The mapping can be consulted at any time during its retention by a suitably authorised person. Such a person may be:
  - A member of the authority, *e.g.* in the course of supporting the user in question;
  - An authorised representative of an RP which is relying on the authority, in the course of investigations of incidents or support. Any such inquiry is a Recorded Event.

  The authority should take care that the data protection requirements are fulfilled. It may be appropriate for the CA to provide a mail forwarding mechanism which contacts the subject without revealing the subject's identity.

3.1.4 Rules for interpreting various name forms

Names are X.500 names. Each DN shall contain at least one CN entry. DNs should follow IGTF guidance; and a CSR submitted with the name "backwards" should have its DN reordered upon issuance.

3.1.5 Uniqueness of names

Names used in personal credentials must be unique in the sense that each DN satisifes precisely one of the following:

- The DN is associated with a single

3.1.6 Recognition, authentication, and role of trademarks

3.2 Initial identity validation

The Subscriber who submits a Request must prove the following:

1. possession of the private key;

2. the Subscriber's association with the Request;
3. the validity of the assertions made in the Request;
4. the validity of the implicit assertions made by the issuance of a certificate, if any, including
5. their eligibility to manage a certificate of the requested type, if applicable; and
6. the link to any previous certificate(s) being changed, renewed, or rekeyed, or which is otherwise used as part or all of a proof of any of these claims, and, in particular,
7. for CAs that guarantee Uniqueness and for Requests which are Certificate Requests, that the Subscriber is the owner of all other certificates issued by the same CA with the same DN as the one in the Request.

- It is the responsibility of the RA Operator to validate these claims prior to the approval of a Request for a certificate.
- It is the responsibility of the Subscriber to provide Information sufficient to validate these claims to the RA Operator, and to give the RA Operator permission to Process the Information.
- Proofs associated with verifying claims 1-3 should be held in an auditable form by the RA or the CA for as long as any certificate associated with this Information is Valid.
- Proof of possession of certificates from other CAs may, at the discretion of the CA, be accepted as partial or full proofs of any or all of these claims. In this case, the Assurance of the certificate(s) thus provided shall be considered.

3.2.1 Method to prove possession of private key

Possession of private key is proved when required by either

- Signing a relevant document: certificate request, email, or similar, which is linked to the request.
- By issuing a challenge which can be responded to successfully with, and only with, access to the private key.

3.2.2 Authentication of organization identity

There is in general no authentication of organisational identity for EEs. While organisations typically have their own RA(s), the approval of a CSR by an RA must not be construed as an assertion that the Subject is a member of the same organisation. For RAs, organisational identity is verified by the CA via letters signed by departmental authorities on headed paper.

3.2.3 Authentication of individual identity

Each Subject must be uniquely identified. It is the responsibility of the Subscriber to present information to the RA which is adequate and sufficient to establish the identity of the Subject. The Subscriber must have the authority to grant the RA the right to process the relevant data according to the rules defined by this document and any additional applicable document. By giving the RA the information, the Subscriber grants this right to the RA and issuing authority for the duration required by this document.

3.2.4 Non-verified subscriber information

Certificates may contain non-verified information about the Subject. Each CPS compliant with this policy shall describe which information in the certificate is non-verified.

3.2.5 Validation of authority

Validation of authority is required for RAs. This authority is granted via the RA's organisational role.

3.2.6 Criteria for interoperation

Each CA shall aim to maximise the interoperation for purposes required by the RPs, by following applicable guidelines for the profile of the certificates, and by providing the associated services required to support the these purposes.

3.3 Identification and authentication for re-key requests

Rekey requests must be signed by the private key corresponding to the certificate whose rekey is being requested.

Before approving the rekey of a Medium assurance certificate, the RA Operator must be able to assert that the information contained in the certificate or implied by the possession of the certificate is still correct. It is the responsibility of the Subscriber to supply any Information required to complete the validation of the request.

Before approving the rekey of a High assurance certificate, the RA Operator must re-check all Information as for an initial request. It is the responsibility of the Subscriber to supply any Information required to complete the validation of the request.

A certificate which is not Valid may be rekeyed if the CA, the RA, and the Subscriber can establish the continued Validity of the assertions explicitly encoded in, or implicitly implied by, the certificate. This check should be done in an auditable way.

3.3.1 Identification and authentication for routine re-key

Identification and authentication for routine re-key is performed either with the proof of possession of the private key, along with a subsequent check that the explicit and implicit data of the certificate is still valid at the time of approval.

3.3.2 Identification and authentication for re-key after revocation

Identification and authentication for re-key after revocation is generally done as for an initial request. However, depending on the type of revocation, if the CA can establish the identity of the user such that this establishment is in an auditable form, it is possible for the CA to re-key the certificate.

3.4 Identification and authentication for revocation request

Any CCR, or any other Request for change of Validity of a certificate, must be either present proof that the circumstances for revocation are fulfilled, or must be authenticated to an RA Operator and validated by the RA Operator.

Any such Request should include the reason for revocation or otherwise change of status, or the RA Operator should be able to determine this reason prior to the approval of the Request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Certificate Requests are submitted by Subscribers. Subscribers are expected to be working with or associated with projects related to UK e-Science, or to other similar scientific and academic information technology activities.

Each CA must document the format required for all types of Requests that it supports, and provide descriptions of processes for submitting these Requests, and any related Information, securely to the CA. The CA must provide implementations, or references to suitable implementations, for the generation, protection, and storage of keys in a trustworthy manner,

4.1.1 Who can submit a certificate application

Certificate applications can be submitted by members of organisations that have RAs, as well as other people who can justify their need for a certificate.

4.1.2 Enrollment process and responsibilities

1. The Subscriber generates a key pair and a CSR;

2. The Subscriber submits the CSR to the CA, along with other required information, such as the type of certificate requested;
3. The relevant RA is notified of the submission;
4. If required, the Subscriber shall provide to the RA the relevant information required for the RA's approval of the Request.
    (a) The The RA shall always verify that the Request was submitted by the Subscriber;
    (b) The RA shall always verify that the Subscriber is authorised to make the Request on behalf of the Subject;
    (c) If the Subject and the Subscriber are the same, the Subscriber is always considered authorised to make the Request, but the Subscriber may still need to prove that they are eligible to hold a certificate of the desired type.
5. When satisfied that the conditions for the approval of the Request are fulfilled, the RA will record the parts of the information that they are required to keep in auditable form, and approves the Request.
6. The CA shall validate the CSR and, if required, any additional information from the RA, and sign the Certificate. Once approved, the CA shall normally sign the Certificate within one working day.
7. The Subscriber shall be notified of the issuance of the Certificate, along with information on how to get it and pair it with the private key.
8. The Subscriber ensures that the Subject of the Certificate

4.2 Certificate application processing

It is the responsibility of the Subscriber to ensure that sufficient Information is submitted to validate the Request. The Information must be submitted to a suitable RA Operator for the Request if the CA has RAs, or to the CA by some other means provided by the CA if the CA does not have RAs.

In either case, the CA or RA may delete Requests which have not been approved after 30 days.

A CA is under no obligation to accept a Request. If a CA rejects a Request, it should provide a reason to the Subscriber. CAs should endeavour to reject incorrect data or malformed Requests as early in the submission process as possible, using automated checks and feedback to Subscribers when possible.

4.2.1 Performing identification and authentication functions

- The Subscriber is responsible for the authentication of the Subject, as described in section 3.2 as well as 3.3.1 and 3.3.2. It is generally the responsibility of the Subscriber to contact the RA to ensure that the identification and authentication process is started.

- The RA is responsible for processing the Request and the information satisfying the requirements of the CA and in compliance with the relevant data protection leglislation.
- The CA is responsible for the timely issuance of the Certificate.
- The Subscriber is responsible for the delivery of the Certificate and private key to the Subject.
- The Subscriber is responsible for the correct management and use of the Credential from the time of its issuance until its revocation or destruction. This period of responsibility extends beyond the expiry of the Certificate unless the private key is destroyed.

4.2.2 Approval or rejection of certificate applications

A CA which requires human intervention for its approval or rejection of requests shall design its processes and training to ensure that such processes are sufficiently rigorous, auditable, and timely.

4.2.3 Time to process certificate applications

A Ca shall generally process its requests within one working day of the receipt of data necessary for the approval from the Subscriber.

4.3 Certificate issuance

It is the responsibility of the IA to issue a certificate whenever a Certificate Request has been approved. These should be issued in a timely manner: for Short Lived certificates, issuance should be essentially immediate; issuance of other EE certificates should be within one working day. If issuance is not immediate, the CA should inform the Subscriber of the issuance.

The CA alone determines the assertions contained in the issued certificate:

- The CA is not required to copy assertions contained in the Request into the certificate.
- If the CA copies assertions from the Request, or from Information associated with the Request, into the certificate, the CA may modify
- The CA may add any assertion appropriate to the intended use of the certificate.
- The CA should aim to make the generated certificate consistent with the use desired by the Subscriber.
- It is the responsibility of the CA to keep any change as described in this section in auditable form. If Information beyond that already held by the CA is required to assert the validity of such a change, then it is the responsibility of the CA to ensure that such Information is recorded and kept in auditable form.

- The CA may notify the RA Operator or the Subscriber of such changes and the reason for such changes, but is under no obligation to do so. If queried by the RA Operator or Subscriber, the CA must provide the reason for the change.

CAs may, but are not required to, publish EE certificates. CA certificates must be public, and published in suitable repositories.

4.3.1 CA actions during certificate issuance

The CA shall:

- Verify any additional data, when applicable, provided by the RA;
- Verify the signature on the CSR;
- Check whether there are outstanding CRRs pertaining to the Certificate if the Request is a renewal or re-key, in which case the CA must perform additional investigations to ensure the correctness of the issuance;
- Sign the Certificate;
- Notify the Subscriber of the issuance.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA notifies the Subscriber of the issuance (or non-issuance, if the request is denied by the CA). This notification must be timely, within (subject to the time of delivery of notification) a short time after the issuance.

4.4 Certificate acceptance

If the issued certificate is a CA certificate, the Subscriber should inspect the certificate upon receipt of the certificate.

A certificate is deemed to be accepted by a Subscriber at the first Use of the certificate, or if the CA has not been notified of any corrections within seven days of issuance of the certificate.

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

The certificate is made available or sent to the Subscriber. There is no requirement on the CA to publish the certificate on the CA's repository, or otherwise, even when the certificate contains public data.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

A certificate may be Used by

- its EE, for any Permitted Purpose of the certificate, provided it is Valid;
- the Subscriber who owns the certificate, if it is Valid, and if it is Invalid under certain other conditions to be defined by the CA, to submit Requests based on the certificate.
- anyone, to revoke it, if the CA supports revocation.

Any other Use of the certificate is prohibited.

A CA must not allow financial transactions to be a Permitted Purpose. Entity authentication is always a permitted purpose of End Entity certificates.

The Permitted Purposes of CA certificates are certificate signing and signing certificate status information. No other Use of CA certificates is permitted.

A certificate must not be Used if its private key is known to be Compromised.

All Permitted Purposes must be expressed according to Best Practices at the time of issuance in the extensions of the certificate.

RPs should note that there is likely to be a certain delay between the circumstances for revocation being fulfilled and the certificate revocation time being timestamped by the IA. If determining whether a given certificate is Valid prior to a known revocation date, the RP should use their own discretion to decide whether to rely on the certificate.

Relying Parties should validate certificates to their satisfaction prior to Reliance. For CAs that publish certificate Validity information, this validation should include a check of the Validity of the certificate, using reasonably fresh Validity data.

Relying Parties must not Use certificates for any purpose which is not a Permitted Purpose.

It is the responsibility of the Subscriber to ensure that private keys are generated, stored, activated, and destroyed according to the current best practices. The Subscriber must ensure that in normal Use of the certificate, only the intended End Entity is able to activate the private key. For non-personal certificates, the Subscriber may designate a backup person.

4.5.1 Subscriber private key and certificate usage

A Subscriber may use the private key for constructing Requests. The Credential may be used by the Subscriber to request revocation, suspension, change, or renewal, or to send signed email to the CA.

The Subject may use the Credential for the purposes defined by the CA.

4.5.2 Relying party public key and certificate usage

A RP may use a certificate for the purposes designed by the CA. If available, RPs should check certificate status prior to Reliance.

4.6 Certificate renewal

Certificates may be renewed if the CA supports renewal. In this case, the Subscriber is notified of the issuance of the new certificate. Acceptance of the certificate is the same as for new certificates.

A CA supporting renewal must specify whether:

- The Subscriber must request renewal of the certificate; and
- The RA Operator must be notified of the renewal and must approve the renewal prior to the issuance of the new certificate.
- Additional Information is required at the time of renewal to approve the renewal, which Information is required, who can supply it, and whether the Information must be auditable.

If the CA has defined a key usage period for the key contained in the certificate, then the certificate must not be renewed if the notAfter date of the renewed certificate exceeds the end of the key usage period. In this case, the CA should not issue a renewed certificate with a lifetime shortened to fit into the remaining key usage period.

Invalid certificates should not be renewed. A certificate must not be renewed if the CA is aware that the one or more Certificate Assertions are invalid. A CA should not renew a certificate if it suspects that one or more Certificate Assertions are invalid, and may investigate further to establish whether the renewed certificate can be issued. A CA may reject any renewal request and request that the Subscriber rekey the certificate.

4.6.1 Circumstance for certificate renewal

If the CA supports it, a certificate may be renewed if it is not a SLCS certificate and it is about to expire. The CA in question shall define this time period: it is generally the time when the Subscriber will receive their first warning about the expiry of the certificate.

For CAs which support certificate renewal, a certificate may be renewed if the issuing CA is satisfied that the conditions for certificate issuance are still satisfied, that the information in the certificate is still correct, and that the private key is sufficiently protected and sufficiently strong to justify its continued use, and has not been unduly exposed in its use prior to the renewal.

If a renewal is based on a renewal request, additional checks will apply (section 4.6.3). A CA may under well-defined circumstances issue a renewed certificate without basing it on a renewal request (section **??**).

Data which is recorded in association with the validation of a new request should also, when re-checked in association of a renewal, be recorded in the same form. In particular, if the data for the initial request is required to be auditable, then so should be the data associated with the renewal.

4.6.2 Who may request renewal

For CAs that support certificate renewal, the Subscriber may request renewal of a certificate, or the CA may issue it automatically, provided adequate checks have been made (section (4.6.1). SLCS certificates must not be renewed.

4.6.3 Processing certificate renewal requests

The processing of a certificate renewal request shall include the following checks:

- That the Subscriber made the renewal request;
- That the certificate to be renewed is not revoked or suspended;
- That the certificate to be revoked does not have pending revocations, unless those pertain to the renewal directly (this will have to be investigated with the Subscriber on a case by case basis);
- That the key is still adequately protected.

4.6.4 Notification of new certificate issuance to subscriber

The Subscriber is notified of certificate issuance by email, or if applicable, by the tool which was used to generate the CSR.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

For CA certificates, the issuance is notified to the relevant repositories and Relying Parties.

4.7 Certificate re-key

Certificates may be rekeyed if the CA supports rekey. In this case, the Subscriber is notified of the issuance of the new certificate. Acceptance of the certificate is the same as for new certificates.

The Subscriber must request rekey of the certificate. The CA must ensure that all certificate assertions are valid before approving the rekey request, possibly via the appropriate RA Operator. If the RA Operator needs additional

Information to perform these checks, then it is the responsibility of the Subscriber to supply it.

A certificate must not be rekeyed if the CA is aware that the one or more Certificate Assertions are invalid. A CA should not rekey a certificate if it suspects that one or more Certificate Assertions are invalid, and may investigate further to establish whether the rekeyed certificate can be issued. A CA may reject any rekeyal request and request that the Subscriber rekey the certificate.

The procedures for notification and acceptance of rekeyed certificates is the same as for new certificates.

4.7.1 Circumstance for certificate re-key

Certificates may be re-keyed if the circumstances for the issuance of the certificate are still valid; if they can be checked in forms which are auditable as required; and if the Subscriber proves possession of the private key; and the private key is not compromised.

4.7.2 Who may request certification of a new public key

The Subscriber may request certification of a new public key. It is noted that the role of Subscriber for a given Subject may have changed.

4.7.3 Processing certificate re-keying requests

As 4.6.3.

4.7.4 Notification of new certificate issuance to subscriber

As 4.6.4.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

As 4.6.6.

4.7.7 Notification of certificate issuance by the CA to other entities

As 4.6.7.

4.8 Certificate modification

CAs may support Certificate Change Requests (CCRs) if it supports revocation. It is the responsibility of the Subscriber (who owns the certificate whose change is being requested) to submit a CCR to the CA. The Subscriber must provide all Information required to validate the change, possibly via the appropriate RA Operator.

Change request should pertain to Certificate Assertions only.

If a CCR is rejected, the CA must notify the Subscriber, stating the reason for rejection.

If a CCR is approved, the CA shall issue a new certificate with its Certificate Assertions about the subject updated accordingly. The CA may implement the change as a renewal or rekey.

The procedures for notification and acceptance of changed certificates is the same as for new certificates.

After the acceptance of the changed certificate, the previous certificate, upon which the change was based, shall be revoked.

4.9 Certificate Revocation and Suspension

The CA may, but does not have to, notify the Subscriber of any change in status of a certificate owned by the Subscriber.

The circumstances for revocation are defined in section **??**.

A reason for revocation should be submitted with every revocation request. The CA must publish the time for revocation, and may publish the reason for revocation. CAs must publish certificate status information also for expired certificates whose Permitted Purposes may require checking the Validity of the certificate at a time other than the present time.

In addition, the following circumstances should lead to either revocation or suspension of the certificate, for CAs that support suspension:

- Suspected compromise of private key associated with the certificate.
- One or more Certificate Assertions is invalid.

Suspension may be used by the CA if it is suspected that a circumstance for revocation is fulfilled, and the CA needs time to investigate.

CAs may implement suspension by, possibly temporarily, revoking the certificate. If so, the CA should provide means to make it clear to a person investigating that the certificate is suspended, rather than revoked, whereas a service will see the certificate as revoked. This policy sets no time limit on the duration of suspension.

CAs should endeavour to process revocation requests as soon as possible. Updated certificate status should be published essentially immediately.

An EE CA which publishes CRLs must publish CRLs with a “lifetime” not less than thirty days. A fresh CRL should be issued at least half the way through the CRL’s “lifetime,” or at least seven days prior to the “expiry” of the CRL, whichever comes first.

4.9.1 Circumstance for certificate modification

For CAs that support certificate modification, certificates may be modified if data in the certificate is no longer correct. (The alternative is revoking the certificate, or (for SLCS) letting expire.)

4.9.2 Who may request certificate modification

The Subscriber or the RA for the Certificate may request modification.

4.9.3 Processing certificate modification requests

Modification requests should be submitted by the Subscriber or the RA; and should be approved by the RA insofar as they pertain to verifiable information, in a form which is auditable if this is required by the CA.

4.9.4 Notification of new certificate issuance to subscriber

As 4.6.4.

4.9.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.9.6 Publication of the modified certificate by the CA

As for other certificates, see 4.6.4.

4.9.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.10 Certificate revocation and suspension

4.10.1 Circumstances for revocation

CAs that support revocation must define the circumstances for revocation. These reasons must include:

- Compromise of the private key associated with the certificate. In this case, it is the responsibility of the Subscriber to submit the revocation request as soon as possible.
- Violation of Subscriber obligations.
- Violation of End Entity obligations.

4.10.2 Who can request revocation

Anyone can submit a request for revocation. The request should include a reason as well as an identification of the Certificate or certificate to be revoked.

4.10.3 Procedure for revocation request

The request will normally have to be checked and approved by an RA; alternatively, if it is can be signed by the private key associated with the certificate, it is automatically approved.

4.10.4 Revocation request grace period

No stipulation.

4.10.5 Time within which CA must process the revocation request

Once approved, a CRR is signed into a CRL the next time the CA signs. Online CAs should issue a fresh CRL within minutes; semi-offline CAs should issue a CRL within one working day. Offline CAs should issue the CRL as soon as possible.

4.10.6 Revocation checking requirement for relying parties

Unless approved by proving possession of the private key, the CRR must be checked by an RA or some similarly authorised person, possibly in collaboration with others, to assess whether the reasons for revocation are fulfilled.

4.10.7 CRL issuance frequency (if applicable)

The CRLs must be issued when a CRR is approved, as defined in section 4.10.5, and otherwise seven days, or earlier, prior to the nextUpdate.

4.10.8 Maximum latency for CRLs (if applicable)

The CRL must be published as soon as it is signed (within fifteen minutes).

4.10.9 On-line revocation/status checking availability

CRLs must be available from the CA's online repository, and may be available from other sources. A CA may provide an OCSP responder. RPs are encouraged to cache and proxy CRLs, for local availability and to ease the load on the CA repository; however, they are encouraged to check for fresh CRLs at least every four hours.

4.10.10 On-line revocation checking requirements

RPs should check the status of a certificate to their satisfaction prior to the reliance on the certificate.

4.10.11 Other forms of revocation advertisements available

No stipulation.

4.10.12 Special requirements re key compromise

No stipulation.

4.10.13 Circumstances for suspension

A CA may implement suspension of certificates. In this case, it shall define the reasons for suspension, which may include:

- The certificate is requested disabled for a certain length of time;
- An investigation into possible suspension is ongoing.

4.10.14 Who can request suspension

Suspension can be requested by

- The Subscriber, in which case it is expected that the suspension request is signed by the private key corresponding to the certificate;
- An RA;
- Other people defined by the CA in collaboration with RPs, *e.g.*, security officers.

4.10.15 Procedure for suspension request

A certificate suspension request is submitted to the CA. If submitted by a suitably authorised person, the request is considered approved, and should be implemented as soon as possible.

4.10.16 Limits on suspension period

No stipulation.

4.11 Certificate status services

Certificates that support certificate status must provide a way to query the status of a certificate. This query may require possession of the certificate, but must not require possession of the private key.

If a CA supports revocation or suspension, it must publish a CRL.

4.11.1 Operational characteristics

Certificate status services should be run on secure services, ideally running no other services other than CA online services, and with sufficient security measures implemented to reasonably prevent and detect the unathorised modification of certificate status.

4.11.2 Service availability

Best efforts should be made to ensure the 24/7 availability of certificate status services, subject only to regular maintenance and security patches.

4.11.3 Optional features

No stipulation.

4.12 End of subscription

The subscription is said to have ended if a certificate:

- has expired, or been revoked, or is otherwise Invalid and is deemed likely to not become Valid at any time in the future; and
- no Request has been submitted based on the certificate, or all such Requests have been rejected.

It is the responsibility of the CA to ensure that personal Information pertaining to the certificate is destroyed following a grace period after the end of subscription. This period must be no less than six months. The period should be no more than three years.

4.13 Key escrow and recovery

Keys (by which hereinafter is understood private keys along with any associated activation data) belonging to Personal Named certificates must not be escrowed.

Other keys may be escrowed by the CA if the CA has generated the keys on behalf of the Subscriber, or by trusted third parties.

A key must not be escrowed if the Subscriber is not aware of this escrow, and the circumstances under which the key may be released and to whom. The CA need not be informed whether the key is escrowed.

4.13.1 Key escrow and recovery policy and practices

No stipulation.

4.13.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Every CA infrastructure should be held in secured locations with access control. While access control may be based on roles or group membership, access should be logged by individual identity.

The Subscriber who obtains a CA certificate is considered the CA Manager. For small CAs, the CA Manager is responsible for the appointment of CA Operators

5.1 Physical controls

5.1.1 Site location and construction

Online CAs shall be hosted in secure locations, with security conforming (or exceeding) those required for the type of CA.

5.1.2 Physical access

Physical access must be limited to authorised system administrators, to CA personnel, and other authorised people.

5.1.3 Power and air conditioning

If the CA is not offline, it should be operated in controlled computing environments.

5.1.4 Water exposures

The CA should describe aim to limit the risk of water exposure, or alternatively should be able to rapidly rebuild itself (within the time requirement for issuance of CRL) if damaged in a water incident.

5.1.5 Fire prevention and protection

Fire prevention and suppression systems should be used, or a disaster recovery process like in section 5.1.4 should be used.

5.1.6 Media storage

All media should be stored appropriately and securely, aiming to compromise between the need to retain the information and the need to keep it confidential and restricted to authorised personnel.

5.1.7 Waste disposal

All media must be wiped or otherwise destroyed before being disposed of. Any media with Personal Data must be destroyed when required by the CA's data protection procedure. In this case, only necessary and sufficient information should be retained to ensure the continued requirements of the CA with respect to the Certificate, *e.g.*, to ensure the uniqueness and non-reuse of the Name.

5.1.8 Off-site backup

Off site backups may be used, or other similar controls, to ensure the DR in case of a disaster in the main building. In this case, as with other backups, the procedure for accessing and unlocking the backup must be carefully documented and independently reviewed.

5.2 Procedural controls

Procedures shall be defined for all operators (RA, CA) involved in the CA's operations.

5.2.1 Trusted roles

The CA shall define roles of all the people involved in the operations. All of these roles are considered trusted, and due processes shall be employed to ensure that the roles are filled by sufficiently trusted personnel.

5.2.2 Number of persons required per task

For most tasks involved in the day to day operations of the CA, a single person in the appropriate role can perform the task (or none, in the case of automated tasks). However, for exceptional tasks such as the activation of an offline CA, or access to a backup, the CA should define n-of-m processes for performing the role where in general it is expected that $n > 1$ and $m \geq 3$.

5.2.3 Identification and authentication for each role

When interacting with a computer system, each operator must authenticate, using either personal certificates, smart cards, or passwords, as appropriate. Passwords alone shall not be used.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

It is expected that persons appointed to the roles defined by the CA are employed by the organisation running the CA. Persons appointed to RA roles are expected to be employed by the organisation that appoints them.

5.3.1 Qualifications, experience, and clearance requirements

No stipulation.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

The appropriate training for the role shall be required,

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

In the case of an operator's unauthorised use of a system, the IT policy of the organisation employing the operator shall apply.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No stipulation.

5.4 Audit logging procedures

Each CA shall self audit once a year.

5.4.1 Types of events recorded

Requests shall be logged, as well as any processing of the requests. In addition, systems logs shall be kept for all systems.

5.4.2 Frequency of processing log

No stipulation.

5.4.3 Retention period for audit log

No stipulation.

5.4.4 Protection of audit log

The logging system should employ best practices to protect the confidentiality of the log data, and to prevent the unauthorised modification or deletion of the log data.

5.4.5 Audit log backup procedures

No stipulation.

5.4.6 Audit collection system (internal vs. external)

Auditing collection system is internal.

5.4.7 Notification to event-causing subject

In the case of an event, the seriousness and potential implications of the event shall be assessed. As an outcome of this assessment, the CA manager shall determine whether and which parties shall be notified of the event. These may include the PMA, RPs, or RP security officers, organisational security officers, auditors, or the TAGs.

5.4.8 Vulnerability assessments

See 5.4.7.

5.5 Records archival

Records pertaining to a Certificate shall be kept for at least three months beyond the expiry of the Certificate.

5.5.1 Types of records archived

Records pertaining to a Certificate shall be recorded. These will include Requests pertaining to a Certificate, as well as emails.

5.5.2 Retention period for archive

No stipulation.

5.5.3 Protection of archive

The data shall be appropriately protected against unintentional disclosure and release to unauthorised people.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

Archive collection is internal.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

A CA shall re-key or extended in a timely manner, such that at least every end entity certificate issued by the CA remains valid during its own lifetime when validated against the CA's Certificate. Additional guidelines from RPs regarding re-key and extension should be followed.

5.7 Compromise and disaster recovery

A CA should have suitable and adequate business continuity and disaster recovery procedures. These must be documented and reviewed at least internally.

5.7.1 Incident and compromise handling procedures

Incident response procedures should involve the relevant security officers of the affected organisations and/or RPs, as appropriate.

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

Standard recovery processes associated with the operation of computing resources at the site shall be employed. These must be documented and reviewed as a part of a self audit.

5.7.3 Entity private key compromise procedures

In the event of compromise, or suspected compromise, of an EE private key, the certificate(s) associated with the key must be requested revoked as soon as possible.

In the event of an authority private key compromise, the process described in section 5.4.8 shall be used.

5.7.4 Business continuity capabilities after a disaster

The CA shall make an assessment of its components which shall include the requirements on availability of the components. The CA shall make a plan for the availability and integrity of the component consistent with the requirement.

5.8 CA or RA termination

In the event of RA termination, the RA is considered expired once its operator status are revoked, and all their credentials have expired. Operators should remain active while Certificates approved by the CA remain valid; if not, the CA shall take over the responsibility of the Certificates which would otherwise have been covered by the RA.

In the case of termination of the CA, the termination shall be made known to RPs in advance, in sufficient time for all EE keys to be replaced, so at least in sufficient timeliness as with a rollover (section 5.6).

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pairs shall be generated using the best practices, with secure random number input, generated (for CA certificates) from a hardware random number device or equivalent.

6.1.2 Private key delivery to subscriber

The Subscriber shall deliver the key to Subject in a suitably secure way, which minimises the risk of exposing the key to unathorised persons, preserves the integrity of the key, and ensures the delivery to the correct Subject.

6.1.3 Public key delivery to certificate issuer

The public key is delivered to the certificate issuer in the CSR.

6.1.4 CA public key delivery to relying parties

No stipulation.

6.1.5 Key sizes

Key sizes should follow IGTF best practices.

6.1.6 Public key parameters generation and quality checking

The choice of parameters should follow IGTF best practices.

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

If a profile is available from the IGTF, it should be followed. If not, RFC5280 should be followed.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA should record whether the EE private key is held in a cryptographic module. CA private keys of online CAs must be held in a cryptographic module conforming to FIPS140-2 level 3, or FIPS140-2 level 2 with additional compensatory controls which brings the assurance level reasonably to level 3.

6.2.1 Cryptographic module standards and controls

For cryptographic modules, the FIPS140-2 standard shall be used.

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

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

The Subscriber is encouraged to make suitably protected backups of private keys whose certificates can be revoked.

The CA private keys shall have backups as a part of their DR processes.

6.2.5 Private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

Private keys may be imported into a module.

6.2.7 Private key storage on cryptographic module

Private keys should not be stored in non-volatile RAM, but should be stored in a way that the encrypted key can be backed up.

6.2.8 Method of activating private key

For an HSM, suitable activation data shall be employed.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

No stipulation.

6.2.11 Cryptographic Module Rating

See section 6.2.

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

Private key activation data for EE keys shall follow IGTF best practice.

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

Online computers shall follow best practices for services connected to the Internet, particularly with respect to monitoring, firewalling, patching, and intrusion detection. Offline computers used for signing for offline CAs shall be booted and run from operating systems stored on read-only media.

6.5.1 Specific computer security technical requirements

No stipulation.

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

No stipulation.

6.7 Network security controls

No stipulation.

6.8 Time-stamping

No stipulation.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

IGTF best practices should be followed.

7.1.1 Version number(s)

IGTF best practices should be followed.

7.1.2 Certificate extensions

IGTF best practices should be followed.

7.1.3 Algorithm object identifiers

IGTF best practices should be followed.

7.1.4 Name forms

IGTF best practices should be followed.

7.1.5 Name constraints

No name constraints shall be used.

7.1.6 Certificate policy object identifier

The certificate shall include OIDs which describe the appropriate policies under which it was issued.

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

No stipulation.

7.2 CRL profile

IGTF best practices should be followed.

7.2.1 Version number(s)

IGTF best practices should be followed.

7.2.2 CRL and CRL entry extensions

IGTF best practices should be followed.

7.3 OCSP profile

For a CA which provides OCSP, IGTF best practices should be followed.

7.3.1 Version number(s)

For a CA which provides OCSP, IGTF best practices should be followed.

7.3.2 OCSP extensions

For a CA which provides OCSP, IGTF best practices should be followed.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

A self audit of the CA's compliance with IGTF shall be carried out annually.

Other audits can be carried out when requested by members of the PMA.

8.2 Identity/qualifications of assessor

A self audit shall be carried out by a person familiar with the operations of the CA.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

The purpose of the audit is to assess compliance with IGTF requirements.

8.5 Actions taken as a result of deficiency

The methodology described in the OGF CAOPS self audit document shall be followed.

8.6 Communication of results

Results are communicated to the PMA and the TAG.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

A CA should not impose fees on its day-to-day operations activities.

9.1.1 Certificate issuance or renewal fees

There shall be no fees associated with certificate issuance or renewal.

9.1.2 Certificate access fees

There are no fees for access to certificates.

9.1.3 Revocation or status information access fees

There are no fees for access to certificate status information.

9.1.4 Fees for other services

A CA may impose reasonable fees for extraordinary requests such as Freedom of Information, Data Protection related requests, and third party audits, in order to cover its costs of processing such requests.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

In general, CAs should be operated by legal organisations with the intention of long term operations, as required by the IGTF charter.

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

A CA which processes personal data has a responsibility to comply with the relevant data protection legislation, following processes described in Appendix C.

Other data considered confidential should be protected according to best practices. The protection of such information should generally be documented in a format suitable for review by security officers and peer CAs.

9.4 Privacy of personal information

See section C.

9.4.1 Privacy plan

See section C.

9.4.2 Information treated as private

All personal data not mentioned in section **??** is treated as private.

9.4.3 Information not deemed private

The representation of the Subject's name encoded in the CN(s) of the certificate is considered public data, even when the certificate itself is not public data.

9.4.4 Responsibility to protect private information

See C.

9.4.5 Notice and consent to use private information

See C.4.

9.4.6 Disclosure pursuant to judicial or administrative process

See C.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

Every CA accredited with the IGTF grants IGTF the non-exclusive rights to distribute in perpetuity the CA certificates it uses as trust anchors, including a path to a self-signed root, along with associated metadata files.

Unless specified otherwise, this document is distributed under the Creative Commons Attribution 4.0 licence (CC BY). Copyright remains with STFC (section 1.5).

Section 9.16.3 contains text derived from, or copied from, the UK Department of Trade and Industry (DTI) supplementary example agreements from the Lambert Working Group on Intellectual Property (as of 2013, with the Intellectual Property Office), and from the DTI Office of Science and Technology LINK CBI/AURIL model collaboration agreement, and are under their original licence.

This document typeset with LaTeX.

9.6 Representations and warranties

No stipulation.

9.6.1 CA representations and warranties

A CA compliant with this profile

9.6.2 RA representations and warranties

No stipulation.

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

A CA compliant with this profile does not accept any liability for financial loss, or loss arising from incidental damage or impairment, resulting from its operation. No other liability, implicit or explicit, is accepted.

9.9 Indemnities

No stipulation.

9.10 Term and termination

No stipulation.

9.10.1 Term

No stipulation.

9.10.2 Termination

In the event that the CA ceases operation, all Subscribers, sponsoring organisations, RAs, and Relying Parties will be promptly notified of the termination.

In addition, all CAs with which cross-certification agreements are current at the time of termination will be promptly informed of the termination.

All certificates issued by the CA that reference this Certificate Policy will be revoked no later than the time of termination.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

9.12 Amendments

This policy may be updated from time to time.

9.12.1 Procedure for amendment

Each CA shall identify the relevant stakeholders to be informed of changes in advance, and shall identify the set of people who shall approve a change, and the means by which such approval is sought.

9.12.2 Notification mechanism and period

Changes to this policy shall be announced at least 30 days in advance for minor changes, and 90 days in advance for major changes.

Amendments to this document which fix typos or clarify statements without being associated with a change in policy need not be announced in advance, but a changelog shall still be kept.

9.12.3 Circumstances under which OID must be changed

The OID must be changed with every policy change. Editorial changes as decribed in section 9.12.2 shall retain the same OID.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

This policy is governed by, and is to be construed in accordance with, English law. The English Courts will have exclusive jurisdiction to deal with any dispute which has arisen, or may arise out of, or in connection with, this policy.

9.15 Compliance with applicable law

Compliance with the Data Protection Act (1998) is described in Appendix C.

9.16 Miscellaneous provisions

The policy described in this document supersedes all previous policies for the UK e-Science CA.

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

STFC may define policies, practices, and processes, and may provide services in collaboration with JANET UK, or may at any time in the future hand over some, or all, responsibilities for policies and/or services, to JANET.

9.16.3 Severability

If any part or any provision of this document shall to any extent prove invalid or unenforceable in law, including the laws of the European Union, the remainder of such provision and all other provisions of this document shall remain valid and enforceable to the fullest extent permissible by law, and such provision shall be deemed to be omitted from this document to the extent of such invalidity or unenforceability. The remainder of this document shall continue in full force and effect and the e-Science CA, Subscribers, and RPs shall negotiate in good faith to replace the invalid or unenforceable provision with a valid, legal and enforceable provision which has an effect as close as possible to the provision or terms being replaced.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.

A Revision History

Version	OID	Date	Comments
0.1		4 September 2001	Initial unapproved release
0.3		30 January 2002	Andrew's changes
0.4		13 March 2002	Jens' changes
0.5		April/May 2002	Tim's changes
0.6		28 May 2002	draft version
0.7	1.1	17 July 2002	final draft
0.8	1.2	10 October 2002	Removed identification by telephone, made specification of host verification more precise, added missing RFC2527 entries.
0.9	1.3	31 March 2003	Update to request extensions.
1.0	1.4	30 October 2003	Describe renewal. Tightened up several parts, including Applicability, personal information stored, etc.
1.1	1.5	04 March 2005	Documented that we use SHA1 to sign.
1.2	1.6	15 May 2005	Documented CA upgrade, Data protection act, and some codifications of existing practice.
1.3	1.7	4 August 2006	CA rollover, signing key online, robots.
1.4	1.8	26 Nov 2007	Security rollover, plus minor security-related updates (only). 2nd update fixed year.
1.5	1.9	03 Feb 2010	1.5 release candidate
1.6	2.0	12 Sep 2011	Rollover;
2.0	2.0	11 Jan 2014	CP presentation to EUGridPMA; Appendices unchanged

The OID in the table is the final two digits of the actual OID, as defined in section 1.2.

B Compliance with Laws and Regulations

The UK e-Science CA operates under English Law. See section **??**.

In the case an RA Operator or CA Operator cannot complete his or her operations without violating rules set forth in this Appendix, the Operator must not complete the operation and must notify the CA Manager, and, if applicable, his or her RA Manager.

C The Data Protection Act

The Data Protection Act 1998 (DPA) [**?**].

C.1 Definitions

- The *data controller* is the CA Manager, the person mentioned in 1.4.2.
- The *data processor* is any RA Manager or Operator.
- The *data subject* is a Subscriber requesting a certificate, or an RA Operator or a CA Operator being appointed as such by the CA.
- *Data* is to be understood as defined in DPA section I.1.
- *Processing* Data is to be understood as defined in DPA section I.1.
- Throughout this Appendix, *Personal Data* means Data which is Personal Data as defined in DPA section I.1 but which is not *Sensitive Personal Data* as defined in DPA section I.2.
- *Personal Information* is defined in section 1.1.1 of this document. For the purposes of the DPA,
  - the photo id is considered Sensitive Personal Data;
  - all other parts of Personal Information are considered Personal Data.

C.2 Preliminaries

The *intent* of Processing Data by the UK e-Science CA is that minimal and adequate Personal Information is stored and Processed in order that the UK e-Science CA may operate according to the policy and practices described in this CP/CPS, including being an internationally approved medium level CA.

C.3 Data

The UK e-Science CA stores the following Data:

1. The CA publishes on its web page, and may publish by other methods, the Subscriber's *certificate* and thus all information contained therein, including the Subscriber's name;
2. The CA logs and stores all Subscriber and RA interactions with the CA's online service, in order to satisfy the requirements of sections 4.5 and 4.6 of this CP/CPS;

3. The RA Operator Processes Personal Information, and possibly other Data, as described in section C.5;
4. The CA stores authorisation information about the RA Manager and Operators sufficient to convince the CA that the RA Manager and Operators satisfy the conditions of section 5.3.1 and that the CA has the RA Manager's assurance that the RA Operator will operate according to this CP/CPS;
5. For host and service certificates, it may be necessary to obtain and store Personal Data that proves to the RA Operator's satisfaction that Subscriber is responsible system administrator for the resource for which the Subscriber requests a certificate, in accordance with sections 2.1.2, 2.1.3, and 3.1.9;
6. It may be necessary to obtain and store Personal Data to prove to the RA Operator's satisfaction that the Subscriber is entitled to a certificate from the UK e-Science CA, cf. section 1.3.3.

Notwithstanding the above, the Data Processed by the UK e-Science CA is subject to the following restrictions:

- The UK e-Science CA must not Process or attempt to Process any Sensitive Personal Data *except* the photo id.
- Personal Data and Sensitive Personal Data must be relevant and adequate for the purpose for which it is Processed.
- The UK e-Science CA must Process Personal Information only as defined in this Appendix, and in accordance with the DPA.

C.4 Consent

By submitting Data to the online CA ([?]), the Subscriber is considered to have given consent that the submitted Data may be Processed by the e-Science CA (there is a notice to this effect on the web page). By presenting Personal Information to the RA Operator, the Subscriber is deemed to have given consent that this information may be Processed according to the purposes described in this document, and stored according to the procedures described in this document (there is a notice to this effect on the web page). By applying for RA Operator or CA Operator status, the RA Operator or CA Operator is deemed to have consented that the CA can Process the Data as described below (there is a notice to this effect in the template appointment letters provided by the CA).

C.5 Processing

The CA permits that Personal Information is Processed as follows:

1. The CA Operator or RA Operator obtains Personal Information or other Data from the Subscriber or from another Operator relevant and adequate for the purposes described below;

2. A photocopy of the Personal Information is made for the purposes described below;
3. The photocopy of Personal Information is subsequently accessed only for the purposes described below;
4. Subscriber's email address is obtained and used only for the purposes described below;
5. Relevant and adequate information is Processed to satisfy section 4.5 of this CP/CPS in accordance with sections 4.5 and 4.6.

C.6 Purpose

The UK e-Science CA Processes Personal Information for the following purposes:

1. Identification of a Subscriber;
2. Subsequent auditing of the Identification process, for the case where the UK e-Science CA must prove the link from the DN to the Subscriber's real identity;
3. Release of Personal Information under the circumstances described in section 2.8 and according to the procedures described in the same section;
4. To maintain the uniqueness of the DN to the extent described in section 3.1.4;
5. For RA and CA Operators, to check to the CA Manager's satisfaction that the RA or CA Operator is duly authorised by appointment letter to operate according to this CP/CPS and that the RA Manager and Operator satisfy the conditions described in section 5.3.1;
6. Adequate Personal Information is Processed to satisfy the auditing requirements set forth in sections 2.7, 4.5 and 4.6 of this CP/CPS;
7. Email address is used only to notify the Subscriber that:
   - A new certificate has been issued to the Subscriber;
   - A certificate held by the Subscriber is about to expire.

Data may be used for statistical purposes

- only with the Data Controller's permission; and
- if there is reasonable cause; and
- if the published information contain neither Personal Data nor Sensitive Personal Data, and no Personal Data or Sensitive Personal Data can be derived from it; and
- the Processing associated with and required for statistical purposes are done in accordance with the DPA section 33.

Any other use of Personal Information is explicitly forbidden.

C.7 Data Release

Circumstances requiring Processing of Personal Information include, but are not necessarily limited to, the following cases:

1. A CA Manager or Operator is considered to have breached CA Obligations (section 2.1.1);
2. An RA Manager or Operator is considered to have breached RA Obligations (section 2.1.2);
3. A Subscriber is considered to have breached Subscriber's Obligations (section 2.1.3);
4. Release of information as described in section 2.8, including any release required by UK law;
5. Release of information as required for auditing purposes, including compliance audit as described in section 2.7.

In each case, the UK e-Science CA shall ensure that only the adequate and relevant information is released and that the information is Processed lawfully and in accordance with the rules of sections C.5 and C.6, and in accordance with the DPA.

C.8 Data Maintenance

There is no requirement for keeping Personal Information Processed by the RA up to date, except to the extent required to satisfy the RA Operator that the information mentioned in 5 and 6 in section C.3 is still valid if and when certificates that required this information prior to their approval are being renewed.

It is the RA Manager's responsibility to ensure that the Data Processed by the CA concerning his or her RA or any Manager or Operator associated with that RA is kept up to date, and inform the CA of any update.

C.9 Data Retention

Personal Information shall be kept by the UK e-Science CA for as long as is necessary:

1. Personal Information used to obtain a personal certificate with a certain DN shall be kept for as long as the Subscriber has a valid certificate with this DN, including renewals of the certificate, and for a period beyond the expiry or revocation of the latest certificate held by the Subscriber necessary to satisfy the retention requirements described in section 4.6;
2. Data used to obtain a host or service certificate shall be kept for as long as the Subscriber is responsible administrator for the resource for which the certificate was obtained, and for a period beyond the expiry or revocation of the latest certificate held by the Subscriber, or beyond the administrator rights being passed on to someone else, necessary to satisfy the retention requirements described in section 4.6.

3. Data used by the CA Manager to authorise RA Managers and Operators must be kept for a period beyond the termination of the RA necessary to satisfy the requirements described in section 4.6. For the termination of the CA, the conditions in sections 4.6.2 and 4.9 apply.

It is the responsibility of the RA Manager to ensure that appropriate technical and organisational measures are taken against unlawful or unauthorised Processing of Data held by the RA. It is the responsibility of the CA Manager to ensure that appropriate technical and organisational measures are taken against unlawful or unauthorised Processing of Data held by the CA.

C.10 Data Termination

It is the responsibility of the RA Manager to ensure that Personal Information held and Processed by the RA is adequately destroyed by the end of the retention period. It is the responsibility of the CA Manager to ensure that Personal Information held and Processed by the CA is adequately destroyed by the end of the retention period.