
Asia-Pacific
Economic Cooperation

# Public Key Infrastructure Guidelines

## Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross-Jurisdiction eCommerce

APEC eSecurity Task Group
APEC Telecommunications & Information Working Group

May 2005

Prepared by:
Mr Steve Orlowski for the eSecurity Task Group
of APEC Telecommunications & Information Working Group

Contact:
eSecurity Team
Department of Communications, Information Technology and the Arts
GPO Box 2154
Canberra ACT 2601
Australia
Tel: (61) 2 6271 1230
Website: www.dcita.gov.au

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org, Website: www.apec.org


APEC#205-TC-03.1 ISBN 981-05-4008-6


Asia-Pacific
Economic Cooperation

# Public Key Infrastructure (PKI) Guidelines

Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross-Jurisdiction eCommerce

APEC Telecommunications & Information Working Group
APEC eSecurity Task Group

May 2005

Prepared by:
Mr Steve Orlowski for the eSecurity Task Group
of APEC Telecommunications & Information Working Group

Contact:
eSecurity Team
Department of Communications, Information Technology and the Arts
GPO Box 2154
Canberra ACT 2601
Australia
Tel: (61) 2 6271 1230
Website: www.dcita.gov.au

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION
SECRETARIAT
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012 Fax: (65) 6775-6013
Email: info@apec.org, Website: www.apec.org


APEC#205-TC-03.1 ISBN 981-05-4008-6

# CONTENTS

# GUIDELINES FOR SCHEMES TO ISSUE CERTIFICATES CAPABLE OF BEING USED IN CROSS JURISDICTION eCOMMERCE

eSECURITY TASK GROUP
APEC TELECOMMUNICATIONS AND INFORMATION
WORKING GROUP

As PKI and eCommerce have evolved a number of jurisdictions have implemented legislation governing electronic transactions and developed (Public Key Infrastructure) PKI schemes. In some cases the legislation requires PKI certificates supporting electronic transactions to meet specified conditions before those transactions have legal effect or before certain legal presumptions apply. While a number of standards and similar documents (such as Internet Engineering Task Force (IETF) Requests for Comments (RFCs)) provide some guidance, they do not necessarily address the requirements for legal effect in some jurisdictions and the issue of cross jurisdiction recognition of certificates. As a result differences between schemes have emerged that can potentially impede cross jurisdiction recognition of transactions and as a consequence eCommerce itself.

The eSecurity Task Group (eSTG) was originally established as the Public Key Authentication Task Force to address this issue in the APEC region. However it was recognised that any approach developed for APEC must also interact with other approaches, particularly those developing in Europe.

To address the issue the eSTG undertook a comparison of a number of existing schemes and tried to identify a class of certificate in each scheme that could potentially be used for eCommerce and then tried to identify common requirements for the issue of those certificates. These certificates could be used in the business to business context for contract formulation, online purchasing and shipping documentation; in the business and citizens to government context for customs and quarantine clearance and taxation, statistical and social security returns; in the business to consumer context such as online purchasing and contract formation, and in the government to government context for exchange of passenger and goods movement information. They are not intended for use for highly sensitive or national security information or for very high value transactions.

The comparison was based on the provisions IETF RFC 2527, which was the current RFC at the time the mapping was undertaken, and involved the following schemes and classes of certificate:

| **Economic Area** | **Scheme Basis or Authority** | **Certificate Class Mapped** |
|---|---|---|
| Australia | Gatekeeper (Australian Government) | Grade 2, Type 2 |
| Canada | Government of Canada PKI | Medium assurance |
| European Union | ETSI QCP - TS 101 456 | Qualified certificate |
| Hong Kong, China | Electronic Transactions Ordinance | Recognized certificate issued by a recognized CA |
| Singapore | Electronic Transactions Act | Certificate issued by a licensed CA |
| United States | Federal Bridge Certification Authority | Medium assurance |

As a result of the comparison two sets of guidelines for schemes issuing certificates for cross jurisdictional eCommerce have been drafted. These guidelines also take it account the work of the PKI Interoperability Expert Group and the two surveys of PKI practices that it undertook. The guidelines attempt to identify the most common approaches used in the schemes compared.

The guidelines have also been aligned with the ***Guiding Principles for PKI-based Approaches to Electronic Authentication*** developed by the PKI Interoperability Expert Group and adopted at APEC TEL27. These guiding principles are set out below.

***GUIDING PRINCIPLES FOR PKI-BASED APPROACHES TO ELECTRONIC AUTHENTICATION***

*APEC member economies are encouraged to take the following Principles into consideration when establishing either voluntary or regulated PKI schemes. They are intended to facilitate inter-jurisdictional acceptance of foreign certification authorities (CAs) and the development of cross-jurisdictional recognition arrangements for this purpose. In this regard, they provide only the basis however, as a detailed mapping of all policy, legal and technical aspects is required in order for cross-certification to occur.*

*These Principles are also intended to help provide guidance to member economies in establishing their authentication policies and assist those with existing policies to identify and address potential deficiencies in their approach.*

*Finally, it should be noted that, while these Principles have been developed for the PKI environment, they should not be interpreted as advocating any one technology solution over another. Rather, they focus attention on considerations in the PKI environment in view of the predominant role played by public-key cryptography in the electronic authentication marketplace.*

***I. LEGISLATIVE/LEGAL FRAMEWORK***

- *The development of frameworks that set out parameters for the establishment and operation of certification authorities (CAs) can facilitate cross-jurisdictional acceptance of the services they provide.*

- *Such frameworks should allow for the acceptance of services originating in other jurisdictions.*

- *The establishment of legislative and legal frameworks that give legal effect to documents and signatures in electronic form produced by both domestic and foreign CAs will facilitate legal predictability on a cross-jurisdictional basis.*

- *Such frameworks should not unduly require the use of particular technologies. In addition, they should allow for changing market standards, developments in existing technology and the introduction of new technology.*

***II. POLICY FRAMEWORK***

- *Requirements for the institutional standing of CA service providers (including capital and financing requirements for the establishment and operation of CAs) can generate public trust and confidence and facilitate cross-jurisdictional recognition of certificates issued by those CAs.*

- *Assessment schemes that utilise recognised standards and best practice to ensure technical interoperability between participants can facilitate cross-jurisdictional recognition of certificates.*

- *The implementation of widely accepted technical standards and management in PKI assessment schemes can allow for CAs to be assessed.*

- *Policies and procedures for cross-jurisdictional recognition of PKI assessment schemes can facilitate legal predictability and certainty in respect of certificates issued under those schemes.*

***III. OPERATIONAL FRAMEWORK (PERTAINING TO CA OPERATIONS)***

*General*

- *The use of the widely adopted Internet X.509 framework IETF/ RFC 2527 for the Certificate Policy (CP) and Certification Practice Statement (CPS) will facilitate cross-jurisdictional recognition.*

*Certificate Registration and Validation*

- *The establishment of processes for registration and initial identity validation that are fit for purpose and take into account those processes used in other jurisdictions will facilitate cross-jurisdictional recognition of certificates.*

*Key Management*

- *The use of key escrow of signature keys can undermine user confidence and impede cross-jurisdictional recognition of certificates.*

- *The use of best practices derived from internationally recognized sources when performing key generation will facilitate cross-jurisdictional recognition of certificates.*

- *The adoption of international best practice that confidentiality and signature key pairs should be different will improve user confidence and facilitate cross-jurisdictional recognition of certificates.*

*Cryptographic Engineering*

- *The use of internationally recognized cryptographic algorithms of sufficient cryptographic length and strength will facilitate interoperability and cross-jurisdictional recognition of certificates.*

- *Ensuring that cryptographic keys and algorithms are sufficiently strong to protect the cryptographic result from attack for the term of validity of the certificate (e.g. should not exceed 5 years) will increase security and facilitate the cross-jurisdictional recognition of certificates.*

- *The assessment of cryptographic processes to a minimum level of FIPS 140-1 Level 3 or equivalent will facilitate cross-jurisdictional recognition of certificates.*

*Distinguished Names*

- *The use of accepted best practice for standardizing the contents of Distinguished Names Components in the certificate will facilitate interoperability.*

- *In particular, the use of standard X.509 extensions such as the Policy OID to represent the intended applicability of the digital certificate will facilitate cross-jurisdictional recognition.*

*Directory Standards*

- *The use of the most commonly used international directory standards such as the X.500 Directory Service or LDAP (lightweight directory access protocol) v3 will facilitate interoperability of PKI applications*

*Systems and Operations*

- *The use of international best practices for personnel security control and physical security control will enhance security and facilitate the cross-jurisdictional recognition of certificates.*

- *The use of at least dual controls for the operation of CA services and processes (e.g. CA private key control and management) will facilitate cross-jurisdictional recognition of certificates.*

- *The use of guidelines for systems and software integrity and control that are compliant with FIPS, the Common Criteria or equivalent recognised standards will enhance security and facilitate the cross-jurisdictional recognition of certificates.*

- *Establishment of archival policies that ensure the retention of relevant material for a sufficient minimum duration (e.g. a minimum of 7 years) will facilitate the cross- jurisdictional recognition of certificates.*

- *The use of time stamps and security mechanisms to prevent any intentional changes to archival records such as the use of hashes should be advocated to facilitate cross- jurisdictional recognition of certificates*

- *Ensuring that the general-purpose repository and certificate revocation list (CRL) are generally available when required will develop user confidence and facilitate cross-jurisdictional recognition of certificates.*

- *Ensuring that facilities are generally maintained to receive and act on requests for suspension when required will develop user confidence and facilitate cross-jurisdictional recognition of certificates.*

*Management Guidelines*

- *Establishment of business continuity and disaster recovery planning provisions will develop user confidence and facilitate cross-jurisdictional recognition of certificates.*

- *The establishment of provisions or guidance in the event that a CA discontinues will develop user confidence and facilitate cross-jurisdictional recognition of certificates.*

*The use of compliance audits/assessments by an independent party as part of security best practice for accreditation or licensing will develop user confidence and facilitate cross-jurisdictional recognition of certificates.*

The guidelines, which have been prepared to assist economies without schemes to develop schemes that are potentially interoperable and to assist those economies with schemes in any review of the interoperability of their schemes, are set out below together with a model for schemes accrediting certification authorities.

It should be noted that schemes may also cover other classes or types of certificates than those for use in cross jurisdiction eCommerce. These guidelines are not intended to address those other certificates nor are they intended to limit schemes to only issuing certificates covered by these guidelines.

The first set, *Guidelines for Operation of a Certification Service Provider Accreditation Scheme*, addresses the structure and role of a CSP accreditation scheme (**Scheme Management** in the model) and apply whether or not a scheme operates a Certification Authority (CA). The second set, *Guidelines for the Certificate Policy and Certification Practices Framework for Issuing Certificates Capable of Being Used in Cross Jurisdiction eCommerce* addresses the provisions of the Certificate Policy (CP) and Certification Practice Statement (CPS) of the elements of the operations of Certification Service Providers (CSPs) accredited under the scheme (**Certification Authority Operations** in the model). Where a CSP does not undertake the full activities of a CA, such as a separate Registration Authority (RA), only the provisions relating to its operations would apply.

While the guidelines can cover schemes that operate a Certification Authority that issues certificates to CAs accredited under the scheme and to other schemes and accredited CAs recognised by the scheme, they do not require a scheme to operate its own CA. Where a scheme does operate a CA, the CP and CPS for that CA should align with the second set of guidelines. Where a scheme does not operate a CA the second set of guidelines would not apply to the scheme administrators and its facilities. However the scheme would still need to take the provisions into account in developing its policies and when assessing CAs for accreditation under the scheme.

Separation of the guidelines into two sets can allow multiple schemes to adopt a common implementation of the certificate policy and certification practices guidelines while adopting separate implementations of the CSP accreditation scheme guidelines.

The US Federal PKI Certificate Policy Working Group has developed a methodology for providing a judgement as to the equivalence between elements of policy based around the framework defined in RFC 2527. This methodology was used in a comparison mapping between the US Federal Bridge Medium Assurance Certificate Policy and the European Qualified Certificate Policy as defined in European Telecommunications Standards Institute Technical Specification TS 101 456.

The methodology identifies four degrees of equivalence between RFC 2527 policy provisions in the schemes being compared:

- Equivalent – The provisions are equivalent,
- Comparable – Whilst there are differences in the provision this does not significantly impact on the security achieved,
- Partial – There is partial mismatch between the policy provisions,
- Missing – The policy does not address this provision

Through this methodology it is possible to identify areas where there is mismatch that requires attention in deciding whether cross recognition is possible. This methodology could be used when mapping different schemes or mapping a scheme against these guidelines.

Legislative/legal frameworks

The guidelines are based on RFC 3647 which addresses policy and technical aspects of PKI. RFC 3647 does not address the legislative/legal framework to support electronic commerce and transactions including PKI. In 1997, the then APECTEL Public Key Authentication Task Group made a deliberate decision not to develop guidelines for legal frameworks, choosing instead to rely on the United Nations Commission on International Trade Law (UNCITRAL) work in developing model laws for electronic commerce and electronic signatures. Most economies have used these models in developing their legislation.

A number of APEC economies have implemented electronic commerce or electronic transactions legislation. In all cases that legislation, either explicitly or implicitly, allows the use of PKI. In some cases the legislation and supporting instruments set out specific requirements for legal recognition of electronic transactions and electronic signatures.

At APEC TEL27 the eSecurity Task Group adopted *Guiding Principles for PKI-based Approaches to Electronic Authentication* that are set out above. These principles noted that *Such* [Legislative/Legal] *frameworks should allow for the acceptance of services originating in other jurisdictions.* They also noted that *Policies and procedures for cross-jurisdictional recognition of PKI assessment schemes can facilitate legal predictability and certainty in respect of certificates issued under those schemes.*

Some economies' legislation includes provisions for the accreditation of CAs within the jurisdiction and either accreditation or recognition of accreditation of CAs outside the jurisdiction. In other economies legislation does not regulate the accreditation of CAs, including those in other jurisdictions. Where legislation does not regulate the accreditation of CAs, schemes can set their own criteria for accreditation of CAs, including foreign CAs. These guidelines are designed to assist both regulated and voluntary approaches through common provisions for assessment and accreditation.

Cross-Jurisdiction Interoperability

Different economies have taken different approaches to interoperability of CAs within their jurisdictions. These approaches include establishment of root CAs, cross certification between CAs, establishment of bridge CAs, issue of scheme accreditation certificates to CAs and provision of trust status information. These various approaches are addressed in the APEC Report *Electronic Authentication – Issues relating to its selection and use*[1].

The issue is how these interoperability approaches can be extended across jurisdictions. The APEC approach to this problem is for recognition to occur at the scheme level rather than the individual CA level. Thus where a scheme recognises another scheme, it automatically recognises any CAs accredited under the scheme. Recognition would be based on assessment of the other scheme's accreditation process rather than assessing each individual CA accredited by the other scheme. These guidelines are designed to assist in the assessment of a scheme's accreditation process to establish an equivalent or greater level of assurance. Where schemes issue multiple classes of certificates, the cross recognition process involves identifying a class of certificate acceptable for use in both jurisdiction and basing the assessment on that class of certificate.

Where no scheme is operating in a jurisdiction, or some sectors of s jurisdiction, these guidelines can assist in any cross recognition arrangement between a scheme in one jurisdiction and individuals CAs in the other jurisdiction.

In 2000 the then APECTEL Electronic Authentication Task Group developed the concept of cross-recognition which can be defined as

> *an interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to authenticate a subject in the other PKI domain, and vice-versa.*

Such authority information is typically the result of either a formal CA licensing or accreditation process in the economy of the other PKI domain, or a formal compliance audit process performed on the representative CA of the PKI domain. Technically, the information can be stored as the value of a certificate field accessible by the relying party or can be evidenced by an electronic accreditation certificate. Other approaches include the establishment of signed certificate trust lists, signed directories of cross certificates or trust status information servers.

Where a subscriber certificate contains sufficient information to allow a relying party to either establish a certificate path to the required trust anchor, or establish the location of the required trust status information, the different approaches should not prevent certificate validation.

[1]http://www.apec.org/apec/publications/all_publications/telecommunications.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/workinggroups/telwg/pubs/2003.Par.0002.File.v1.1

Where CA accreditation and cross jurisdiction recognition information is not made available electronically, automated certificate validation will not be possible. This problem could be addressed, in part, by requesting that a scheme with which a cross recognition agreement is established issue electronic recognition information for each individual accredited CA in the non-electronic scheme, in addition to information on the scheme itself.

# GLOSSARY OF TERMS

A description of the elements of a PKI assessment scheme, including terminology, follows this Glossary

Definitions followed by [RFC3647] have been taken from Internet Engineering Task Force RFC 3647 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework*[2]. In some cases an extended definition, including examples, appears in the RFC

| TERM | DEFINITION |
|---|---|
| **Activation Data** | Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share). [RFC3647] |
| **Archive** | (noun) A long term repository for certificates, certificate revocation lists, public keys and other status information that may be required to validate a transaction at a later date.<br><br>(verb) To place information in an archive (noun). |
| **Assessment (or Compliance Audit)** | The process of measuring the extent of compliance of an entity's operations against high level requirements of the entity and/or scheme, as documented in policies, practices and procedures.<br><br>Assessment(or compliance audit) is a different process to evaluation and generally does not involve a detailed re-examination of hardware and software that has been previously evaluated. |
| **Authentication** | The process of establishing that individuals, organizations, or things are who or what they claim to be. [RFC3647] |
| **CA-Certificate** | A certificate for one CA's public key issued by another CA [RFC3647] |
| **Certificate** | Digital information that binds a subject to a public key in accordance with the scheme. |
| **Certificate Life** | The maximum period for which a certificate may remain valid. |
| **Certificate Lifecycle** | The process of issuance and subsequent classification of a certificate and its associated keys. |
| **Certificate Policy (CP)** | A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. [RFC3647] |
| **Certificate Re-Key** | The process of changing the key pair bound to an entity or subject by a certificate issued under the scheme. This normally entails issuing a new certificate containing the new public key. |
| **Certificate Renewal** | The process of extending the binding between a subject and the associated public key, generally where a certificate has reached, or is about to reach, the end of its life cycle. |

[2] http://www.ietf.org/rfc/rfc3647.txt?number=3647

| TERM | DEFINITION |
|---|---|
| **Certificate Revocation** | The process whereby a certificate is cancelled by a Certification Authority prior to its expiration date and removed from the directory of valid certificates or the status information for the certificate is changed from valid to revoked. |
| **Certificate Revocation List (CRL)** | A list of revoked certificates, including the time and date of revocation, maintained in a repository accessible by potential relying parties. |
| **Certificate Suspension** | The process whereby a certificate is suspended by a Certification Authority prior to its expiration date and temporarily removed from the directory of valid certificates or the status information for the certificate is changed from valid to suspended. |
| **Certificate Trust List** | A list of certificates, generally digitally signed by the issuing authority, used by relying parties to assess whether or not to trust a certificate or a certification path. |
| **Certification Path** | An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path. [RFC3647] |
| **Certification Practice Statement (CPS)** | A statement of the practices that a Certification Authority employs in issuing, managing, revoking, and renewing or re keying certificates. [RFC3647] |
| **Certification Service Provider** | An entity providing services in respect of the issue of certificates – including Certification Authorities, Registration Authorities, Certificate Manufacturing Authorities, Time Stamping Authorities, certificate status information providers and Repository Service Providers.<br><br>NOTE: Some standards use the term Trust Service Provider. However in the context of these guidelines a scheme could be considered to be a Trust Service Provider even if it does not issue certificates. For this reason the term Certification Service Provider has been adopted for entities providing services in respect of the issue of certificates. |
| **Certification Service Provider Accreditation** | Formal declaration by a scheme's Competent Authority that a Certification Service Provider has met the requirements to provide the designated service within the scheme. |
| **CPS Summary (or CPS Abstract)** | A subset of the provisions of a complete CPS that is made public by a CA. [RFC3647] |
| **Cross Certificate** | A certificate issued by one CA to another CA evidencing a trust relationship between the issuing CA and the subject CA. Certificates can be uni-directional or bi-directional.<br><br>Cross certificates can be used to evidence a cross recognition agreement between schemes. |
| **Cross Certification** | The process whereby a CA issues a cross certificate evidencing that |

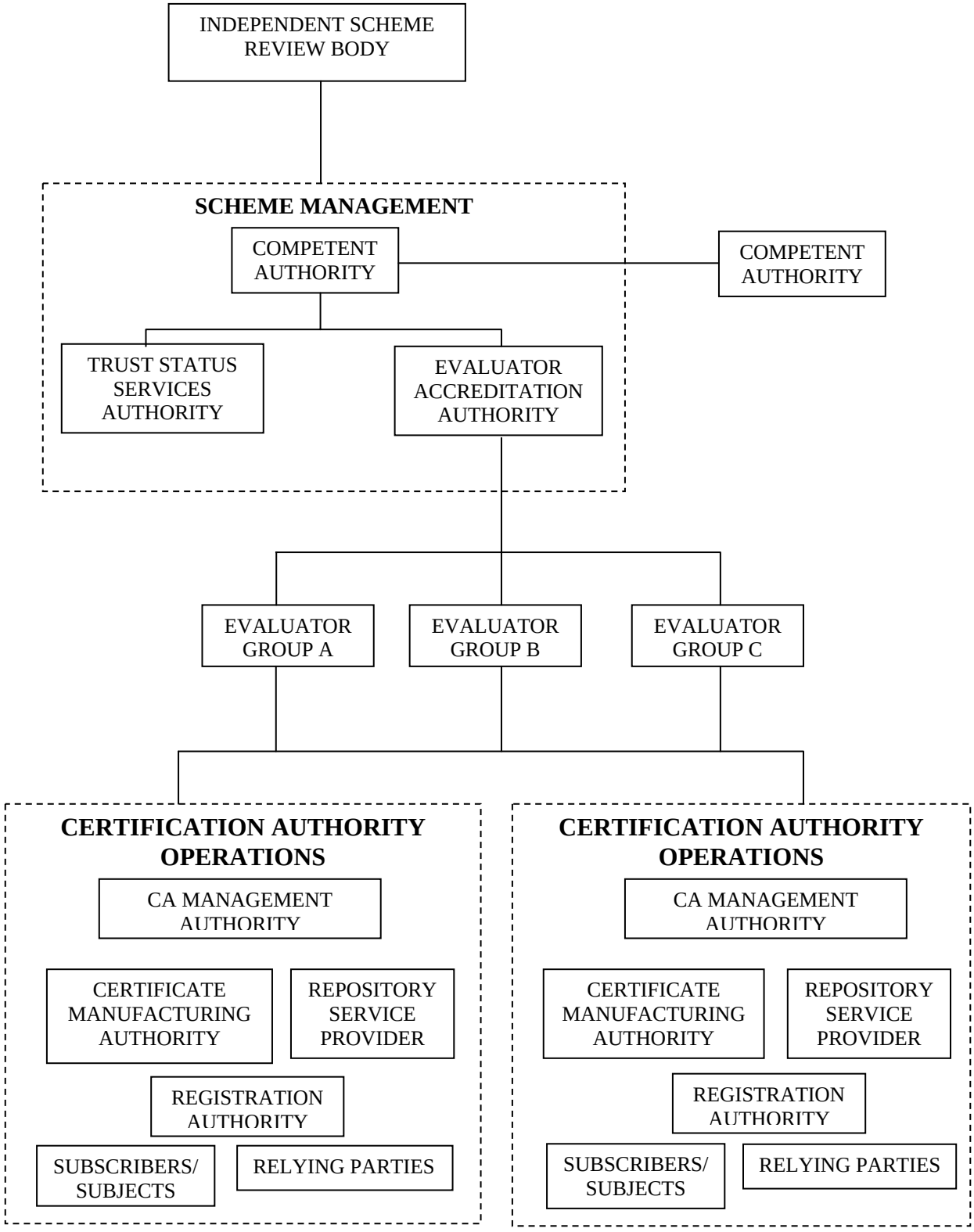
| TERM | DEFINITION |
|---|---|
| | the subject CA operates at an equivalent or higher level of trust to the issuing CA. |
| **Cross Recognition** | An interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to authenticate a subject in the other PKI domain, and vice-versa. |
| **Directory** | A database containing information on certificates issued by a Certification Authority.<br><br>NOTE: In some implementations the terms “Directory” and “Repository” are used interchangeably. In these guidelines the term “Repository” (see below) has a wider scope than the term ”Directory”. |
| **Electronic Delivery** | The process whereby applications, keys or certificates are provided to a subscriber or entities using electronic methods such as e-mail, secure download or dedicated link |
| **Evaluation** | The process of measuring the extent of compliance of an entity’s operations against high level requirements of the entity and/or scheme objectives and documented policies, practices and procedures and measuring the extent of compliance of an entity’s hardware and software with the requisite protection profile.<br><br>NOTE: In some contexts the terms “evaluation”, “certification” and “accreditation” have specific meanings. Within these guidelines the term “evaluation” is as defined above; the term “certification” relates to the process of binding a public key to a subject; and the term “accreditation” relates to the process whereby a Competent Authority declares that a Certification Service Provider meets the requirements of, and is authorised to operate as part of, the scheme. |
| **Identification** | The process of establishing the identity of an individual or organization, i.e., to show that an individual or organization is a specific individual or organization. [RFC3647] |
| **Identity Re-Validation** | A repeat of the process of identification. |
| **Identity Re-Validation Period** | The maximum period for which identification or identity re-validation remains valid. |
| **Issuing Certification Authority (Issuing CA)** | In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject Certification Authority) [RFC3647] |
| **Key Usage Period** | The maximum permitted usage period for a key pair, generally based on an assessment of the key pair’s vulnerability to compromise. |
| **Other Relevant Documentation** | Documentation other than a Certificate Policy or Certification Practice Statement that documents objectives, polices, practices, procedures and arrangements relevant to the operation of the scheme and entities accredited under the scheme. |

| TERM | DEFINITION |
|---|---|
| | It could include:<br>CSP accreditation criteria;<br>security policies;<br>privacy plans;<br>operations manuals; and<br>contracts.<br>These documents need not necessarily be publicly available. |
| **Participant** | An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity. [RFC3647] |
| **PKI Disclosure Statement (PDS)** | An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS. [RFC3647] |
| **Policy Qualifier** | Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information. [RFC3647] |
| **Relying Party Agreement (RPA)** | An agreement between a Certification Authority and relying party that typically establishes the rights and responsibilities between those parties regarding the verification of digital signatures or other uses of certificates. [RFC3647] |
| **Repository** | A collection of information relating to certificates including one or more of:<br>Directories;<br>Certificate Revocation Lists;<br>Certificate Status Information; and<br>Archives<br>NOTE: In some implementations the terms “Directory” and “Repository” are used interchangeably. In these guidelines the term “Directory” (see above) has a narrower scope than the term ”Repository”. |
| **Revocation Grace Period** | The period following an event requiring revocation within which the person requesting revocation should make or confirm a revocation request |
| **Subject** | Entity identified in a certificate as the holder of the private key associated with the public key given in the certificate |
| **Subscriber** | Entity subscribing with a Certification Authority on behalf of one or more subjects and may vouch for some of the subject identification data. |

| TERM | DEFINITION |
|---|---|
| **Subject Certification Authority (Subject CA)** | In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate (see also Issuing Certification Authority). [RFC3647] |
| **Subscriber Agreement** | An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates. [RFC3647]<br><br>NOTE: In some cases a Subscriber may sign a Subscriber Agreement on behalf of a number of Subjects – both natural persons such as employees and machines operated by the Subscriber. |
| **Trust Status Information** | Information provided by a trusted entity such as a scheme's competent authority, that establishes the trustworthiness of certificates issued under the scheme or other recognised schemes. |

## A MODEL FOR CERTIFICATION SERVICE PROVIDER ACCREDITATION SCHEMES

The following is a model for certification service provider accreditation schemes.. The model uses a number of concepts and definitions drawn from RFC 3647 issued by the Internet Engineering Task Force which has superseded RFC 2527.



## GUIDELINES FOR OPERATION OF A CERTIFICATION SERVICE PROVIDER ACCREDITATION SCHEME

| | GUIDELINE |
|---|---|
| Scope of Scheme | The scope of the scheme can be public, government, sector or organisation specific.<br><br>This model is designed for certificates supporting domestic or international electronic commerce where there are no contractual arrangements governing authentication services.<br><br>NOTE: A scheme may also support higher or lower levels of certificates. In those cases, the certificates to which this model applies should be identified. |
| Implementation | Implementation can be either mandatory or voluntary within the issuing jurisdiction. |
| Legislative Support | Where the scheme is governed by legislation this should be recorded.<br><br>Where the certificates issued under the scheme confer specific legal effect or presumptions this should be recorded as well as the applicable legislation. |
| Scheme Management | Scheme Management can involve the following elements:<br><br>• Competent Authority;<br>• Evaluator Accreditation Authority; and<br>• Trust Status Services Authority.<br><br>In some implementations several of these elements may be carried out by a single body. |
| Competent Authority | An agent of the legal jurisdiction or community of interest. It is responsible, within the jurisdiction or community, for a number of actions that could include some or all of the following:<br><br>• Defining the policy and legal environment within which the CSP accreditation scheme must operate;<br>• Negotiating with other Competent Authorities to ensure harmonisation across differing legal jurisdictions;<br>• Issuing licenses, authorisations, regulations or other government or legal recognition to various CSPs, including other schemes;<br>• Setting minimum policy requirements for advancing CSP accreditation schemes across differing legal jurisdictions and communities of interest;<br>• Giving formal recognition to standards, criteria and frameworks for advancing the compatibility of CSP accreditation approaches across differing legal jurisdictions;<br>• Approving and giving formal recognition to the CSP accreditation approach;<br>• Operating a Trust Status Service for example through cross certification, Bridge CA or trust status server; and<br>• Giving formal recognition to an *Evaluator Accreditation Body*, which is chartered to carry out the accreditation of *Evaluators* |
| Evaluator Accreditation Authority | An independent body, industry association or other agency which could be recognised by the *Competent Authority* or could function on the basis of trust relationships with *Evaluators* or *CA Management Authorities*. Responsibilities could include:<br><br>• Approving and giving formal recognition that *Evaluators* are professionally competent to perform evaluations of compliance to appropriate policies or other requirements which may be provided by the *Competent Authority*; and<br>• Liaising with the *Competent Authority* on the effectiveness of policy |

| | GUIDELINE |
|---|---|
| | compliance, evaluation guidance, criteria and standards. |
| Trust Status Services Authority | A body, generally part of the scheme, that publishes information or certificates on CAs and other schemes accredited or recognised by the scheme. This information could include information on legal status of a transaction using a certificate issued by a CA or scheme recognised by the scheme. It will generally adopt one of the following approaches:<br><br>• A scheme operated CA that issues certificates to recognised or accredited CAs and schemes;<br>• A Bridge CA that issues cross certificates to recognised CAs within the scheme and to Accreditation, Root or Bridge CAs of other schemes;<br>• A Root CA that issues certificates to recognised or accredited CAs including cross certificates with other Root or Bridge CAs of recognised schemes;<br>• A Trust Status Server that issues certified trust status information on recognised or accredited CAs and schemes and could include a directory of cross certificates with recognised CAs and Accreditation, Root or Bridge CAs of recognised schemes; and<br>• A Trust Status List that lists the CAs and schemes recognised by the scheme which may be digitally signed and may contain the public keys of recognised CAs and schemes. |
| Scheme Operations | Scheme Operations can involve the following elements:<br><br>• Independent Scheme Review Body; and<br>• Evaluators.<br><br>These elements should not be combined as the Independent Scheme Review Board may be required to review the activities of evaluators. |
| Independent Scheme Review Body | An entity or group of entities appointed to review the operation of the scheme. The review would typically be undertaken on establishment of the scheme, and during the schemes operation, in accordance with the terms of the Independent Scheme Review Body. The responsibilities of the Scheme Review Board could include:<br><br>• Assessing whether the scheme generates the required level of trust and meets the objectives of the scheme;<br>• Assessing the operations of the elements of the scheme including those of the *Trust Status Services Authority* and the *Evaluator Accreditation Authority*;<br>• Assessing the scheme's compliance with relevant laws of the jurisdiction in which the scheme operates;<br>• Assessing the scheme's compliance with the policies, practices and objectives of any organisational structure of which the scheme is a part – eg that a government operated scheme complies with government policy, practices and objectives;<br>• Reviewing cross recognition arrangements to ensure they meet the required level of trust for the scheme; and<br>• Publishing all or part of its findings for reference by interested parties. |
| Evaluator | An independent agent, member of an accounting body, financial institution or other qualified professional that is trusted by the *CA Management Authority*. *The Evaluator Accreditation Authority* could formally recognise an evaluator, if such an entity existed in that jurisdiction or community of interest. A number of specialist evaluators could be used in the evaluation of a single *CA Operation*. Responsibilities could include:<br><br>• Evaluating the *CA Operation's* compliance to the CA policy as outlined in its |

| | GUIDELINE |
|---|---|
| | CP, CPS and other relevant documentation such as the CA security policy;<br>• Using specific evaluation guidance, criteria and standards sanctioned by the *Evaluator Accreditation Authority*, to determine that –<br>  • there are adequate controls in place; and<br>  • these controls are operating effectively, such that reliance can be placed on transactions that are recorded, processed, executed or maintained by the elements of the *CA Operations* in question.<br>• Evaluating other evidence of compliance with the CP, CPS and other relevant documentation, where the parties have effected obligations through mechanisms such as contracts and membership agreements and through the implementation of related operational safeguards or business methods. For specific policy requirements, an external reference may be sufficient to convey an understanding to the *Evaluator***,** of the relevant material practices of the domain;<br>• Producing a *CA Operations* Compliance Evaluation Report. The potential users of an evaluation report include:<br><br>a. *Relying parties* have a significant interest in knowing that a scheme's practices operate with sufficient effectiveness to achieve the requirements within the Certificate Policy;<br>b. *Subscribers* have an interest in knowing that the CA is meeting the requirements of the Certificate Policy;<br>c. *Competent Authorities* – An evaluation is an important component of any authorisation, regulation, licensing or other recognition process. The *Competent Authority* could utilise the evaluation report as part of the initial and on-going recognition process; and<br>d. *CA Management Authorities* are a primary user of the evaluation report, as the evaluation is one of the requirements of the Certificate Policy and it demonstrates CA compliance with that policy. The evaluation report could also be used by *CA Management Authorities* in any cross-certification negotiations; and<br>e. *Registration Authorities, Certificate Manufacturing Authorities and Repository Service Providers***.** While the evaluation report is not intended to provide recommendations for improvement in the internal controls of a CA or certification authority, a value-added benefit of the CA compliance evaluation would often include observations of the evaluator for improvements in operations. |
| CA Operations | CA Operations can involve the following elements:<br>• CA Management Authority (generally referred to as the Certification Authority);<br>• Certificate Manufacturing Authority;<br>• Registration Authority;<br>• Repository Service Provider;<br>• Subscriber/Subject; and<br>• Relying Party.<br>In some implementations several of these elements may be carried out by a single body.<br>In most cases, all elements of the CA domain or enterprise must be accredited to establish the required level of trust for a particular certificate. |
| CA Management Authority | A member of the CA domain or enterprise. The CA Management Authority is responsible for the overall operations of the CA and bears ultimate responsibility to Subscribers and Relying Parties who utilise the CA services and to the Competent Authority. Responsibilities could include: |

| | GUIDELINE |
|---|---|
| | • Requesting CA Accreditation under the scheme including CSPs supporting the CA operations;<br>• Selecting and/or defining documentation for use in the CA domain or organisational enterprise;<br>• Establishing appropriate arrangements, eg contracts, with other participants within the CA domain including definition of roles and responsibilities;<br>• Approving practices which the CA must follow by reviewing the<br>• CPS and other relevant documentation to ensure consistency with the CP;<br>• Providing policy direction to other participants;<br>• Generating or requesting the CA signing key; and<br>• Approving any cross-certification or interoperability agreements with external domains;<br>• A CA Management Authority will be unique to a CA operation however there may be multiple CA domains within a CA operation issuing different types/classes of certificates.<br><br>This is the entity identified in a certificate as the certificate issuer. |
| Certificate Manufacturing Authority | A member of one or more CA domains or enterprises within the scheme. Responsibilities could include:<br><br>• Processing requests for certificates from Registration Authorities<br>• Generating or validating subject keys<br>• Generating and signing subject certificates<br>• Processing revocation or suspension requests<br>• Generating and signing directories and CRLs<br>• Generate cross certificates on behalf of the CA domain<br><br>A Certificate Manufacturing Authority may be accredited by the scheme to provide services to multiple CA Management Authorities. |
| Registration Authority | A member of one or more CA domains or enterprises within the scheme. Responsibilities could include:<br><br>• The identification and authentication of certificate applicants;<br>• The approval or rejection of certificate applications;<br>• Initiating certificate revocations or suspensions under certain circumstances;<br>• Processing subscriber/subject requests to revoke or suspend their certificates; and<br>• Approving or rejecting requests by subscribers to renew or re-key their certificates.<br><br>Registration Authorities, however, do not sign or issue certificates.<br><br>A Registration Authority may be accredited by the scheme to provide services to multiple CA Management Authorities. |
| Repository Service Provider (also known as Directory Service Provider) | A member of one or more CA domains or enterprises within the scheme. Responsibilities could include:<br><br>• Publishing and maintaining directories and certificate revocation lists including archives;<br>• Providing certificate validation services;<br>• Providing evidence of date and time against information in the repository; and<br>• Publishing cross certificates on behalf of the CA Management Authority.<br><br>A Repository Service Provider may be accredited by the scheme to provide services |

| | GUIDELINE |
|---|---|
| | to multiple CA Management Authorities. |
| Subject | An entity that is identified in a certificate as the holder of the private key associated with the public key given in the certificate. Responsibilities and obligations of the Subject would be as required by the CA's policy. |
| Subscriber | An entity that enters into an agreement with a CA on behalf of one or more Subjects with the intention of having the CA issue certificates in the Subjects' names. A Subscriber may vouch for some of the Subject identification data. Responsibilities and obligations of the Subscriber would be as required by the CA's policy |
| Relying Party | May or may not be a Subscriber of the same domain. The Relying Party is a recipient of a certificate who acts in reliance on that certificates and/or digital signatures verified using that certificate. |
| CSP Accreditation Criteria | The CSP accreditation criteria for the scheme should be documented and made available electronically for Subscribers and Relying Parties. |
| CSP Accreditation Approval | CSP accreditation approval and the currency of that approval should be published in a manner accessible by Subscribers and Relying Parties. |
| Limitations | Limitations on the use of certificates issued under the scheme should be published electronically and referenced in certificates issued under the scheme. |
| Foreign Certification Services | The scheme should record whether foreign service providers can participate in the scheme and if so any conditions that may apply.<br><br>Under federal and multi-national governments, it is possible that schemes may be established on a state or provincial basis. In these cases the scheme should record whether extra territorial service providers can participate in the scheme and if so any conditions that may apply.<br><br>Similarly for sector or organisational specific schemes the scheme should record whether non-members can provide services and if so under what conditions. |
| Acceptance of Foreign Certificates | The scheme should record whether certificates issued under other schemes, be they foreign or not, will be accepted within the scheme and if so any limitations or conditions that may apply. |
| Use Outside Jurisdiction | The scheme should record whether certificates can be used outside the scheme and if so any limitations that might apply both in respect of the certificates themselves and service provided by Certification Service Providers within the scheme. Limitations may vary from service provider to service provider within the scheme. |
| Cross Certificates | The scheme should record whether cross certificates are supported by the scheme and if so any conditions that may apply. Cross certificates may be bilateral or unilateral and may operate at the scheme level or at the CA within the scheme level. |

## GUIDELINES FOR THE CERTIFICATE POLICY AND CERTIFICATE PRACTICES FRAMEWORK FOR ISSUING CERTIFICATES CAPABLE OF BEING USED IN CROSS JURISDICTION eCOMMERCE

The guidelines are based on RFC 3647 with references to the corresponding RFC2527 provisions.
RFC 3647 superseded RFC2527 in November 2003.

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 1. INTRODUCTION | 1. INTRODUCTION | |
| 1.1 Overview | 1.1 Overview | The scheme CP, CPS and CSP Accreditation criteria, as applicable, and the CP and CPS of all CAs accredited under the scheme should align with IETF RFC 3647.<br><br>NOTE: Documentation for some established schemes may conform with RFC 2527. In those cases, to facilitate comparisons for cross recognition, consideration should be given to mapping the existing documentation against the RFC3647 provisions using the comparative matrix included in RFC3647. The CP and/or CSP accreditation criteria for the scheme should be documented and published electronically in a manner accessible by subscribers and relying parties. The CPs of CAs accredited under the scheme should also be published in a manner accessible by subscribers and relying parties.<br><br>The CPS or a CPS summary or a PKI Disclosure Statement should be published electronically in a manner accessible by subscribers and relying parties.<br><br>The overall framework of the scheme should be recorded at this level including details of the competent authority, policy and operational authorities and various accreditation/evaluation/auditing bodies. |
| 1.2 Document Name and Identification | 1.2 Identification | OIDs in accordance with ISO assignment of OID Component Value should be used for both scheme documentation and documentation for organisations accredited under the scheme. |
| 1.3 Participants | 1.3 Community and Applicability | Community and applicability can be public, government, sector or organisation specific expressed as per RFC 3647<br><br>Where the scheme is governed by legislation this should be recorded.<br><br>Where the certificates issued under the scheme confer specific legal effect or presumptions this should be recorded as well as references to the applicable legislation.<br><br>Details of recognition of foreign schemes and use outside the scheme should also be recorded. |
| 1.3.1 Certification Authorities | 1.3.1 Certification Authorities | A CA's community and applicability may be narrower than that of the scheme. The CA's CP and CPS should set out the community and applicability for certificates it issues in accordance with RFC 3647.<br><br>Where a CA operates as a root or bridge CA these |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | arrangements should be recorded.<br><br>Where a CA certifies subsidiary CAs, details of these arrangements should be recorded.<br><br>Where part of the CA's operations such as registration or directory services are performed by a separate body, details of these arrangements should be recorded. |
| 1.3.2 Registration Authorities | 1.3.2 Registration Authorities | Where separate RAs are permitted under the scheme this should be recorded.<br><br>The CP and CPS for CAs accredited under the scheme should detail registration arrangements where applicable. |
| 1.3.3 Subscribers | 1.3.3 End Entities | The scheme should identify those who can obtain (subscribers) and use certificates (subjects).<br><br>A CA's community may be narrower than that of the scheme. The CA's CP and CPS should detail the subscribers covered by that CA. |
| 1.3.4 Relying Parties | 1.3.3 End Entities | The scheme should identify those who can rely on the certificates (relying parties).<br><br>A CA's community may be narrower than that of the scheme. The CA's CP and CPS should detail the relying parties covered by that CA. |
| 1.3.5 Other Participants | No Provision | Some schemes permit directory services, or repositories, and/or certificate manufacture services to be outsourced. Where this is the case this should be recorded.<br><br>The CP and CPS for CAs accredited under the scheme should detail directory or repository services and certificate manufacture arrangements where applicable. |
| 1.4 Certificate Usage | 1.3.4 Applicability | The purpose of this model is to establish certificates capable of being used in both domestic and international electronic commerce.<br><br>Where the certificates issued under the scheme are required in order to confer specific legal effect or presumptions this should be recorded as well as references to the applicable legislation. |
| 1.4.1 Appropriate Certificate Usage | 1.3.4 Applicability | The appropriate usage of certificates issued under the scheme should be recorded in accordance with RFC 3647. In particular appropriate usage in electronic commerce should be recorded.<br><br>In some cases the appropriate usage of certificates of a CA accredited under the scheme may broader or narrower than that of the scheme itself. The CA's CP and CPS should detail the appropriate usage of its certificates in accordance with RFC 3647. |
| 1.4.2 Prohibited Certificate Usage | 1.3.4 Applicability | The prohibited usage of certificates issued under the scheme should be recorded in accordance with RFC 3647. In |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | particular prohibited usage in electronic commerce should be recorded.<br><br>In some cases the prohibited usage of certificates of a CA accredited under the scheme may broader than that of the scheme itself. The CA's CP and CPS should detail the prohibited usage of its certificates in accordance with RFC 3647.<br><br>In some cases usage for some purposes may not be supported without being specifically prohibited. Limitations to supported usage should be recorded in the same way as prohibited usage. |
| 1.5 Policy Administration | 1.4 Contact Details | |
| 1.5.1 Organization Administering the Document | 1.4.1 Specification Administration Organization | Contact details for those responsible for administration of the scheme should be recorded in accordance with RFC 3647.<br><br>Contact details for CAs accredited under the scheme should be recorded in the CA's CP and CPS in accordance with RFC 3647. |
| 1.5.2 Contact Person | 1.4.2 Contact person | Contact details for the scheme should be recorded in accordance with RFC 3647.<br><br>Contact details for CAs accredited under the scheme should be recorded in the CAs CP and CPS in accordance with RFC 3647. |
| 1.5.3 Person Determining CPS Suitability for the Policy | 1.4.3 Person Determining CPS Suitability for the Policy | Contact details for the person responsible for determining CPS suitability for the policy of the scheme should be recorded in accordance with RFC 3647.<br><br>Contact details for CAs accredited under the scheme should be recorded in the CAs CP and CPS in accordance with RFC 3647. |
| 1.5.4 CPS Approval Procedures | 8.3 CPS Approval Procedures | Where a scheme operates a CA, its procedure for approval of the CPS for the scheme CA should be documented.<br><br>The CPS of a CSP accredited under the scheme should be approved by the scheme. Other relevant documentation should be reviewed by the scheme. Where "commercial-in-confidence" material is included in that documentation only information sufficient to demonstrate compliance with the requirements of the scheme needs to be provided. |
| 1.6 Definitions and Acronyms | No Provision | The CP, CPS and other documentation of the scheme and of CSPs accredited under the scheme should list definitions of terms used and acronyms in the documentation. RFC 3647 Section 2 provides a number of definitions.<br><br>Whilst not included in RFC 3647; these guidelines suggest adding the following sections to the CP and CPS:<br><br>10 Bibliography |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | 11 Acronyms & Abbreviations<br><br>12 Glossary |
| 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES | 2.1.5 Repository Obligations<br><br>2.6 Publication and Repository | <u>Repository</u><br><br>The Repository responsibilities should be recorded in the CA CP and CPS. If the Repository operates as a separate entity, its responsibilities should also be recorded in the documentation of the Repository. The CA and the scheme should record their responsibilities for the operations of the Repository.<br><br>The Repository responsibilities should be recorded in accordance with RFC 3647.<br><br>In addition to responsibilities under the scheme, the CA and the Repository may be subject to legal obligations in both the jurisdiction in which the scheme, CA or Repository is located or in which a transaction utilising a certificate issued under the scheme takes place. These obligations may include legislation covering electronic transactions and privacy.<br><br>In particular the CA and the Repository should ensure that relying parties are aware of their responsibilities and any CA or Repository limitations on liability prior to their utilising the Repository.<br><br>The CA and the Repository should ensure that data relating to the subject/subscriber, relying party or transaction obtained at the time of using the service is collected and protected in accordance with the requirements of the scheme, the CP and CPS and privacy legislation in the jurisdiction or jurisdictions in which the CA and the Repository operate.<br><br>The CA or Repository should ensure that the Repository is available for a high proportion of the time when relying parties might need to access it. It should also ensure the Repository is accessible using access protocols and technologies commonly used by potential relying parties.<br><br><u>Publication</u><br><br>The scheme should publish its CP and/or other relevant documentation.<br><br>The scheme should ensure that details of CSPs accredited under the scheme and the status of that accreditation are available to all subscribers and relying parties including potential subscribers and relying parties.<br><br>CSP accreditation and status can be evidenced by listing on a website, establishing a repository of certificates or public keys of accredited bodies or the issue of certificates, including cross certificates or the issue of certificates or cross certificates. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | Where the use of certificates issued by CAs accredited under a scheme confers particular legal status or presumptions for transactions using those certificates these details should also be published.<br><br>ETSI TS 102 231 "Harmonized TSP status information" can be used to standardise the format of trust status information.<br><br>To minimise the possibility of tampering with repositories, the contents can be digitally signed by the scheme.<br><br>Where the scheme issues certificates or signs the contents of repositories the public key associated with that signing should be published.<br><br>Where a scheme recognises certain categories of certificates issued by other schemes details of that recognition and any limitations that may apply should be published.<br><br>Evidence of recognition of other schemes should be published in the same way as evidence of the status of CAs accredited under the scheme. However the scheme should also provide a link to the location of status information for CAs issued under the other scheme.<br><br>Where a scheme has restricted membership publication can be restricted to that membership |
| 2.1 Repositories | 2.6.4 Repositories | Accredited CAs or RSPs should establish repositories that allow subscribers and relying parties to ascertain the status of certificates issued by a CA accredited under the scheme.<br><br>The repositories should be capable of interoperating with other repositories established under the scheme and under other schemes recognised by the scheme.<br><br>Repositories should be accessible using commonly available protocols and technologies. |
| 2.2 Publication of Certification Information | 2.6.1 Publication of CA Information<br><br>8.2 Publication and Notification Policies | The scheme should publish its current CP, CPS or other relevant documentation on its website. Procedures for access to previous versions should also be published on the website.<br><br>The scheme should provide links to the CP, CPS and/or other documentation of CSPs accredited under the scheme on its website where the approval or status is notified.<br><br>Where a scheme recognises other schemes it should provide links to the CP or other relevant documentation on its website where the existence of a recognition arrangement is notified.<br><br>A CSP accredited under the scheme should publish its current CP, CPS or other relevant documentation on its website. Procedures for access to previous versions should also be published on the website.<br><br>Where publication of some information in the |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | documentation may be prejudicial to the security or operation of the scheme that information may be omitted although its existence should be noted.<br><br>An accredited CA may publish its public key in addition to any publication or dissemination by the scheme itself.<br><br>A CA may publish any certificates relating to its accreditation or any cross certificates with other CAs subject to the rules of the scheme. |
| 2.3 Time or Frequency of Publication | 2.6.2 Frequency of Publication<br><br>8.2 Publication and Notification Policies | The CP and other documentation of CSPs should be published as soon as reasonably possible following modification of the information contained in the documentation taking into account any approval requirements. CSP accreditation and trust status information should be published whenever a change occurs. Procedures for access to previous versions should also be published.<br><br>Certificates should be published promptly following generation and issue taking into account any privacy legislation. Where a repository also includes status information that repository should be published with the same frequency as if it were a CRL.<br><br>A CRL or delta CRL should be published at least once in every 24 hour period. This provision does not apply for CAs, including scheme CAs, who only issue certificates to subordinate, cross recognised or cross certified CAs. |
| 2.4 Access Controls on Repositories | 2.6.3 Access Controls | Access to repositories should be restricted to legitimate subscribers and relying parties taking into account any privacy issues. This provision may not apply for CAs whose certificates are designed for fully open use and whose subscribers have been advised that no access restrictions to repositories will apply.<br><br>Access and other controls should ensure that specific authorisations are required to implement searches of the directory other than validation of a specific certificate.<br><br>Access and other controls should prevent the unauthorised modification or deletion of published material and the contents of repositories.<br><br>NOTE: Uncontrolled directory searches can lead to problems such as establishing the relationship between old and new information where certificates have been modified (a privacy issue) or denial of service attacks. |
| 3. IDENTIFICATION AND AUTHENTICATION | 3. IDENTIFICATION AND AUTHENTICATION | The scheme should record in its CP or other relevant documentation the requirements for identification of individuals and businesses by accredited CAs or RAs, including identity re-validation requirements.<br><br>Where machine and/or attribute certificates are supported the process for binding a certificate with a machine or attribute should be recorded. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 3.1 Naming | 3.1 Initial Registration | The scheme should record the naming conventions to be used in its CP or other relevant documentation.<br><br>The scheme should ensure that CAs or RAs accredited under the scheme have a name claim dispute resolution procedure. |
| 3.1.1 Type of Names | 3.1.1 Types of Names | The scheme should require unique names to be recorded as defined in X.501.<br><br>In some circumstances the use of pseudonyms may be permitted in which case they also should be unique names. |
| 3.1.2 Need for Names to be Meaningful | 3.1.2 Need for Names to be Meaningful | The scheme may permit, in certain circumstances, such as pseudonyms or machine identities, the use of names that may only be meaningful to the intended relying parties. This does not mean that the subject name associated with a pseudonym has to be revealed. |
| 3.1.3 Anonymity or Pseudonymity of Subscribers | 3.1.2 Need for Names to be Meaningful | The scheme may support the use of pseudonyms or machine identities. This does not mean that the subject name associated with a pseudonym has to be revealed. Anonymous subject certificates should not be supported. Anonymous attribute certificates may be supported. |
| 3.1.4 Rules for Interpreting Various Name Forms | 3.1.3 Rules for Interpreting Various Name Forms | The scheme should ensure that the rules for interpreting name forms are available to relying parties. |
| 3.1.5 Uniqueness of names | 3.1.4 Uniqueness of Names | Distinguished names must be unique for each subject of a certificate issued by a CA accredited under the scheme.<br><br>The scheme should ensure that all CAs accredited under the scheme have a unique name for operations within the scheme.<br><br>NOTE: This may be an issue where a single CA seeks accreditation under several schemes. |
| 3.1.6 Recognition, authentication and role of trademarks | 3.1.5 Name Claim Dispute Resolution Procedure<br><br>3.1.6 Recognition, Authentication and Role of Trademarks | The scheme should record in its CP or other relevant documentation whether trademarks can be used and if so the process for ensuring entitlement to use that trademark. |
| 3.2 Initial Identity Validation | 3.1 Initial Registration | The scheme should specify in its CP or other relevant documentation the requirements for initial identity validation. The period after which the initial identity information will require re-validation should be notified to the subject or subscriber. |
| 3.2.1 Method to prove possession of private key | 3.1.7 Method to prove possession of private key | Where a scheme allows subscriber generation of key pairs the subscriber should be required to demonstrate the ability to sign a message, or data, verifiable using the public key submitted for inclusion in the certificate. This data could be a Certificate Signing Request.<br><br>Where a CA generates a key pair on behalf of a subscriber, the subscriber should be required to confirm possession of |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | the private key by signing a message, or data, verified by the associated public key. This step need not apply where the key is provided to the subscriber or subject by a means that ensures only the intended recipient can access the key and the recipient acknowledges receipt of the key. |
| 3.2.2 Authentication of Organization Identity | 3.1.8 Authentication of Organization Identity | A scheme may permit the issue of certificates to organisations.<br><br>Where an organisation applies for a certificate the applicant should be required to provide evidence of the existence of the organisation as well as establishing their authority to act in the name of the organisation.<br><br>Consideration should be given to requiring the applicant on behalf of the organisation to establish their individual identity.<br><br>Where an organisation applies for an identity certificate for a machine associated with the organisation the process for registration of an organisation should be followed.<br><br>Where an organisation intends to associate attribute certificates with its organisation certificate the CA, the scheme and any potential users of those certificates should be advised of the process used to confirm entitlement to that attribute and any limitations on the use of the attribute. In some cases the organisation issuing the attribute certificate may be an accredited CA in which case the information should be included in the CP of that CA. |
| 3.2.3 Authentication of Individual Identity | 3.1.9 Authentication of Individual Identity | Applicants for individual certificates should be required to provide evidence of identity at least equivalent to that required to obtain a passport, national identity card or equivalent government issued photographic identity document. This will generally require the personal attendance of the applicant. |
| 3.2.4 Non-Verified Subscriber Information | No Provision | Where non verified subscriber or subject information is permitted in the registration process this should identified in the scheme, CA and RA CP, CPS and other relevant documentation.<br><br>Non-verified subscriber or subject information should not generally be included in identity certificates.<br><br>In circumstances such as the commencement of a scheme or admission of a large group of subscribers or subjects to the scheme it may not be practicable to follow the initial registration process. In these cases the issue of certificates based on established trustworthy relationship between the scheme, CA or RA and the subject may be permitted.<br><br>In these circumstances consideration should be given to confirmation of the registration on the basis of the normal registration processes as soon as practicable. |
| 3.2.5 Validation of Authority | 3.1.9 Authentication of Individual Identity | Where an individual applies for a certificate evidencing a specific authority, the applicant should be required to |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | provide evidence establishing that authority, including authority to act in the name of an organisation. |
| 3.2.6 Criteria for Interoperation | 4.1 Certificate Application | The scheme should document the criteria for other schemes or CAs to interoperate with the scheme (cross-recognition). This should include the means of evidencing the cross-recognition status such as cross-certificates or other trust status information. |
| 3.3 Identification and Authentication for Re-Key Requests | 4.5 Routine Re-key<br><br>3.3 Re-key after Revocation | The scheme should record in its CP or other relevant documentation the process for identification and authentication of re-key requests from subscribers and CSPs accredited under the scheme. This would include re-keying of cross certificates where appropriate.<br><br>A new certificate certifying the new public key is issued.<br><br>The scheme should also specify in its CP or other relevant documentation any identity re-validation requirements. |
| 3.3.1 Identification and Authentication for Routine Re-Key Requests | 3.2 Routine Re-key | Routine re-key is a scheduled process whereby a new key pair is certified due to the expiration, or anticipated expiration of the current key pair. The scheme should permit subscribers to apply for a routine re-key using their current valid key pair.<br><br>Where the subject keys have expired the initial identification process should be followed.<br><br>The scheme should record in its CP or other relevant documentation the process for routine re-key of CAs accredited under the scheme and the reissue of subject certificates affected by that re-key.<br><br>Where a scheme operates a CA that issues a certificate to accredited CAs, the processes for reissue of certificates to those CAs and their subscribers following a routine re-key of the schemes CA should be recorded in the schemes CP or other relevant documentation.<br><br>Notification of the re-key should be included with status information for the CA. |
| 3.3.2 Identification and Authentication for Re-Key After Revocation | 3.3 Re-key after Revocation | Where the subject keys have been revoked the initial identification process should be followed.<br><br>Where an accredited CA's key has been revoked the scheme should document the process for re-key of the CA and the reissue of certificates to subscribers of that CA.<br><br>Where a scheme operates a CA that issues a certificate to accredited CAs, the processes for reissue of certificates to those CAs and their subscribers in the event of the scheme CA's key being revoked should be recorded in the scheme's CP or other relevant documentation.<br><br>Notification of the re-key should be included with status information for the CA. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 3.4 Identification and Authentication for Revocation Request | 3.4 Revocation Request | The scheme should record the process for requesting revocation of either an accredited CA's key or that of a subscriber or subject of an accredited CA.<br><br>This should include recording the classes of persons who can make a request and the process for verifying the identity of the person making the request and their entitlement to make that request. |
| 4. CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS | 4. OPERATIONAL REQUIREMENTS | A certificate life cycle should not exceed the identity re-validation period specified under the scheme. Confirmation of identity information relating to a certificate such as current operation of an organisation, current business name registration or current domain name ownership may be undertaken within a certificate life cycle without the need to issue new certificates. |
| 4.1 Certificate Application | 4.1 Certificate Application | The scheme should record in its CP or other relevant documentation the minimum processes to be followed for handling of applications for certificates under the scheme.<br><br>The scheme should require completion of a subscriber agreement at the time of application. |
| 4.1.1 Who Can Submit a Certificate Application | 4.1 Certificate Application | The scheme should record in its CP or other relevant documentation the classes of persons or organisations that can apply for certificates. A CA accredited under the scheme may elect to accept applications from only some of these classes, in which case those classes should be recorded in the CP of the CA.<br><br>An RA accredited under the scheme may accept certificate applications on behalf of a CA accredited under the scheme.<br><br>The scheme should allow a subscriber to make applications in respect of multiple subjects where a relationship between the subscriber and subject permitting such action is evidenced. |
| 4.1.2 Enrolment Process and Responsibilities | 2.1.3 Subscriber Obligations<br><br>4.1 Certificate Application | The scheme should record in its CP or other relevant documentation the minimum processes to be followed for enrolment of subscribers and the subscriber responsibilities<br><br>A subscriber or subject should be required to comply with subscriber responsibilities set out by the scheme or in the CP and CPS of the CA.<br><br>The subscriber should be required to sign an agreement to meet their responsibilities and those of subjects enrolled by the subscriber. The agreement should include any consequences of failure to comply with the agreement.<br><br>Where legislation places certain obligations on subscribers or subjects to ensure the legal effect of transactions utilising certificates issued by the CA the subscriber agreement should record those obligations.<br><br>Where a jurisdiction places obligations on subscribers to, or subjects of, schemes outside that jurisdiction those |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | obligations should be made available to those subscribers or subjects.<br><br>Where an RA processes certificate applications on behalf of a CA the scheme should require that the request for certificate manufacture and issue be forwarded in a secure manner. |
| 4.2 Certificate Application Processing | 4.1 Certificate Application<br><br>4.2 Certificate Issuance | The scheme should record in its CP or other relevant documentation the minimum processes to be followed for handling of application of certificates under the scheme. |
| 4.2.1 Performing Identification and Authentication Functions | 4.1 Certificate Application<br><br>4.2 Certificate Issuance | The scheme should record in its CP or other relevant documentation the minimum processes to be followed for performing identification and authentication functions for applications for certificates issued under the scheme. Identification and authentication functions may be performed by a CA or an RA accredited under the scheme.<br><br>Where an RA processes certificate applications on behalf of a CA the scheme should require that the request for certificate manufacture and issue be forwarded in a secure manner.<br><br>If applications are forwarded electronically the scheme should require that the RA has undertaken the required identification processes and that the application be digitally signed by the RA using a key certified by the CA or another authority recognised by the CA.<br><br>Where an RA accepts applications on behalf of a CA, the scheme and CA should ensure that appropriate records are retained by the RA, or another party recognised by the scheme and CA practices, or forwarded to the CA.<br><br>The scheme should permit electronic issue of certificates and keys provided separate trusted channels are used for issue of the certificate and keys and an activation code for the certificate and keys. |
| 4.2.2 Approval or Rejection of Certificate Applications | 4.1 Certificate Application<br><br>4.2 Certificate Issuance | The scheme should record in its CP or other relevant documentation the circumstances under which certificate applications should be accepted or rejected. A CA may elect to include other circumstances for rejection in its CP or other relevant documentation. |
| 4.2.3 Time to Process Certificate Applications | 4.1 Certificate Application<br><br>4.2 Certificate Issuance | The scheme should record in its CP or other relevant documentation the minimum time to process applications for certificates under the scheme. |
| 4.3 Certificate Issuance | 4.2 Certificate Issuance | The scheme should record the minimum requirements for certificate issuance in its CP or other relevant documentation. |
| 4.3.1 CA Actions During Certificate Issuance | 4.2 Certificate Issuance | The CA should issue certificates in accordance with minimum requirements set out in the scheme's CP or other relevant documentation.<br><br>The scheme should permit electronic issue of certificates |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | and keys provided separate trusted channels are used for issue of the certificate and keys and an activation code for the certificate and keys. |
| 4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate | 4.5 Certificate Issuance<br><br>4.3 Certificate Acceptance | The scheme should record the minimum requirements for notification of certificate issuance in its CP or other relevant documentation.<br><br>Notification may be by delivery of the certificate to the subscriber or subject accompanied by a statement of issue or by notification of the issuance of the certificate and the process for obtaining the certificate.<br><br>The scheme should permit electronic issue of certificates and keys provided separate trusted channels are used for issue of the certificate and keys and an activation code for the certificate and keys.<br><br>The scheme should record minimum requirements for verification of receipt of a certificate and subsequent publication of that certificate. These procedures may, in part, be met by a subscriber agreement that may have been signed at the time of application and must abide by privacy legislation, where applicable, particularly as it affects certificate publication. |
| 4.4 Certificate Acceptance | 2.1.3 Subscriber Obligations<br><br>4.3 Certificate Acceptance | The scheme should record minimum requirements for acceptance of a certificate and subsequent publication of that certificate. These procedures may, in part, be met by a subscriber agreement that may have been signed at the time of application.<br><br>Where a certificate is delivered electronically the scheme should require the recipient of a certificate to digitally sign an acceptance message using the keys and certificate provided.<br><br>Once a certificate is accepted a subscriber or subject should be required to comply with subscriber or subject responsibilities set out by the scheme or in the CP and CPS of the CA, the subscriber agreement and relevant legislation. |
| 4.4.1 Conduct Constituting Certificate Acceptance | 4.3 Certificate Acceptance | Certificate acceptance may be evidenced by formal acceptance or by use of the certificate in accordance with the scheme.<br><br>Where a certificate is not accepted within a specified time frame, or is rejected by the subject or subscriber, it should be immediately revoked. |
| 4.4.2 Publication of the Certificate by the CA | 2.1.5 Repository Obligations<br><br>2.6.1 Publication of CA Information<br><br>4.3 Certificate Acceptance | Certificates should be published through a repository accredited under the scheme. The publication procedures should be recorded in the CA's CP and CPS. If the Repository operates as a separate entity, its responsibilities should also be recorded in the documentation of the Repository. The CA and the scheme should record their responsibilities for the operations of the Repository.<br><br>In addition to obligations under the scheme, the CA and the |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | Repository may be subject to legal obligations in both the jurisdiction in which the scheme, CA or Repository is located or in which a transaction utilising a certificate issued under the scheme takes place. These obligations may include legislation covering electronic transactions and privacy.<br><br>The CA and the Repository should ensure that data relating to the subject/subscriber, relying party or transaction obtained at the time of using the service is collected and protected in accordance with the requirements of the scheme, the CP and CPS and privacy legislation in the jurisdiction or jurisdictions in which the CA and the Repository operate.<br><br>The CA or Repository should ensure that the Repository is available for a high proportion of the time when relying parties might need to access it. It should also ensure the Repository is accessible using access protocols and technologies commonly used by potential relying parties. |
| 4.4.3 Notification of Certificate Issuance by the CA to Other Entities | 2.1.5 Repository Obligations<br><br>2.6.1 Publication of CA Information<br><br>4.2 Certificate Issuance<br><br>4.3 Certificate Acceptance | A CA may notify other entities of certificate issuance by direct notification or publication in a repository accessible by the other entity.<br><br>Where an RA processes certificate applications on behalf of a CA, the CA should be notified of issuance and acceptance of that certificate.<br><br>An accredited CA may publish its public key and certificate in addition to any publication or dissemination by the scheme itself.<br><br>A CA may publish any certificates relating to its accreditation or any cross certificates with other CAs subject to the rules of the scheme. |
| 4.5 Key Pair and Certificate Usage | 1.3.4 Applicability<br><br>2.1.3 Subscriber Obligations<br><br>2.1.4 Relying Party Obligations | The scheme should document in its CP or other relevant documentation responsibilities in respect of key pair and certificate usage.<br><br>The purpose of these guidelines is to establish certificates capable of being used in both domestic and international electronic commerce.<br><br>The usage of key pairs and certificates issued under the scheme should be recorded in accordance with RFC 3647. In particular the usage in electronic commerce should be recorded.<br><br>In some cases the usage of key pairs and certificates issued by a CA accredited under the scheme may broader or narrower than that of the scheme itself. The CA's CP and CPS should detail the applicability of its certificates in accordance with RFC 3647.<br><br>Where the certificates issued under the scheme are required in order to confer specific legal effect or presumptions this should be recorded as well as references to the applicable |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | legislation. |
| 4.5.1 Subscriber Private Key and Certificate Usage | 1.3.4 Applicability<br><br>2.1.3 Subscriber Obligations | A subscriber or subject should be required to comply with subscriber or subject responsibilities set out by the scheme or in the CP and CPS of the CA.<br><br>The subscriber should be required to sign an agreement to comply with their responsibilities and those of subjects enrolled by the subscriber. The agreement should include any consequences of failure to comply with the agreement.<br><br>The subscriber or subject responsibilities should be recorded in accordance with RFC 3647<br><br>Where legislation places certain obligations on subscribers or subjects to ensure the legal effect of transactions utilising certificates issued by the CA the subscriber agreement should record those obligations.<br><br>Where a jurisdiction places obligations on subscribers to, or subjects of, schemes or CAs outside that jurisdiction those obligations should be made available to those subscribers or subjects.<br><br>Where a subscriber enters an agreement on behalf of a number of subjects, its responsibilities in respect of the actions of those subjects should be recorded. |
| 4.5.2 Relying Party Public Key and Certificate Usage | 1.3.4 Applicability<br><br>2.1.4 Relying Party Obligations | A relying party should be required to comply with relying party responsibilities set out by the scheme or in the CP and CPS of the CA.<br><br>The relying party should be notified of their responsibilities by way of a PKI disclosure statement or similar document published and made accessible to the relying party. The statement or document should include any consequences of failure to comply with the agreement.<br><br>The relying party responsibilities should be recorded in accordance with RFC 3647.<br><br>Where legislation places certain obligations on a relying party to ensure the legal effect of transactions utilising certificates relied on by the relying party, the documentation should record those obligations. |
| 4.6 Certificate Renewal | 3.2 Routine Re-key<br><br>4.1 Certificate Application<br><br>4.2 Certificate Issuance<br><br>4.3 Certificate Acceptance | A scheme may permit subscribers to apply for a certificate renewal certifying an existing key pair provided the period of the renewed certificate and any previous certificates using that key pair does not exceed the permitted key usage period.<br><br>The scheme should specify in its CP or other relevant documentation any identity re-validation requirements.<br><br>The scheme should record in its CP or other relevant documentation the process for renewal of certificates of CAs accredited under the scheme and the re-issue of subscriber certificates affected by that certificate renewal. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | Where a scheme operates a CA that issues a certificate to accredited CAs, the processes for reissue of certificates to those CAs and their subscribers following renewal of the scheme's CA's certificate should be recorded in the schemes CP or other relevant documentation.<br><br>Notification of the certificate renewal should be included with status information for the CA. |
| 4.6.1 Circumstances for Certificate Renewal | 3.2 Routine Re-key<br><br>4.1 Certificate Application | A scheme should permit subscribers to apply for a certificate renewal certifying an existing key pair provided the period of the renewed certificate and any previous certificates using that key pair does not exceed the permitted key usage period. Certificate renewal is evidenced by the issue of a new certificate and the existing certificate may be revoked or archived. |
| 4.6.2 Who May Request Renewal | 3.2 Routine Re-key<br><br>4.1 Certificate Application | The scheme should record in its CP or other relevant documentation the classes of persons or organisations that can apply for certificate renewal. A CA accredited under the scheme may elect to accept applications from only some of these classes, in which case those classes should be recorded in the CP of the CA.<br><br>An RA accredited under the scheme may accept certificate renewal applications on behalf of a CA accredited under the scheme.<br><br>The scheme should allow a subscriber to make applications in respect of multiple subjects where a relationship between the subscriber and subject permitting such action is evidenced. |
| 4.6.3 Processing Certificate Renewal Request | 3.2 Routine Re-key<br><br>4.1 Certificate Application<br><br>4.2 Certificate Issuance | The scheme should record in its CP or other relevant documentation the minimum processes to be followed for handling of applications for certificate renewal under the scheme.<br><br>The scheme may permit subscribers to apply for a certificate renewal using their current valid key pair.<br><br>A new certificate containing the same subject public key and information as the previous certificate is issued and the existing certificate revoked. |
| 4.6.4 Notification of New Certificate Issuance to Subscriber | 3.2 Routine Re-key<br><br>4.2 Certificate Issuance<br><br>4.3 Certificate Acceptance | The scheme should record the minimum requirements for notification of new certificate issuance in its CP or other relevant documentation.<br><br>Notification may be by delivery of the certificate to the subscriber or subject accompanied by a statement of issue or by notification of the issuance of the certificate and the process for obtaining the certificate.<br><br>The scheme should permit electronic issue of new certificates following certificate renewal.<br><br>The scheme should record minimum requirements for verification of receipt of a new certificate and subsequent |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | publication of that certificate. These procedures may, in part, be met by a subscriber agreement that may have been signed at the time of application for certificate renewal. |
| 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate | 2.1.3 Subscriber Obligations<br><br>3.2 Routine Re-key<br><br>4.3 Certificate Acceptance | New certificate acceptance may be evidenced by formal acceptance or by use of the new certificate in accordance with the scheme.<br><br>Where the new certificate is not accepted within a specified time frame, or is rejected by the subscriber or subject, it should be immediately revoked. |
| 4.6.6 Publication of the Renewal Certificate by the CA | 2.1.5 Repository Obligations<br><br>2.6.1 Publication of CA Information<br><br>3.2 Routine Re-key<br><br>4.3 Certificate Acceptance | New certificates should be published through a repository accredited under the scheme. The publication procedures should be recorded in the CA's CP and CPS. If the Repository operates as a separate entity, its responsibilities should also be recorded in the documentation of the Repository. The CA and the scheme should record their responsibilities for the operations of the Repository. |
| 4.6.7 Notification of Certificate Issuance by the CA to Other Entities | 2.1.5 Repository Obligations<br><br>2.6.1 Publication of CA Information<br><br>3.2 Routine Re-key<br><br>4.2 Certificate Issuance<br><br>4.3 Certificate Acceptance | A CA may notify other entities of new certificate issuance by direct notification or publication in a repository accessible by the other entity.<br><br>Where an RA processes certificate renewal applications on behalf of a CA, the CA should be notified of issuance and acceptance of that new certificate.<br><br>An accredited CA may publish its new certificate in addition to any publication or dissemination by the scheme itself.<br><br>A CA may publish any new certificates relating to its accreditation or any cross certificates with other CAs subject to the rules of the scheme. |
| 4.7 Certificate Re-Key | 3.2 Routine Re-key<br><br>4.1 Certificate Application | Certificate re-key may be scheduled (routine re-key) or may occur following revocation of a certificate.<br><br>The scheme should permit subscribers to apply for re-key using their current valid key pair unless the certificate associated with that key pair has been revoked.<br><br>Where the certificate or key pair has expired, or the information used to verify the identity is no longer valid, the initial identification process should be followed.<br><br>The scheme should record in its CP or other relevant documentation the process for routine re-key, and re-key following revocation of CAs accredited under the scheme and the reissue of subject certificates affected by that re-key.<br><br>Where a scheme operates a CA that issues a certificate to accredited CAs, the processes for reissue of certificates to those CAs and their subscribers or subjects following a routine re-key, or re-key following revocation ,of the schemes CA should be recorded in the schemes CP or other relevant documentation. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | Notification of the re-key should be included with status information for the CA. |
| 4.7.1 Circumstances for Certificate Re-Key | 3.2 Routine Re-key<br><br>4.1 Certificate Application | A scheme should permit subscribers to apply for a certificate re-key certifying a new key. Certificate re-key is evidenced by the issue of a new certificate and the existing certificate may be revoked.<br><br>Where a scheme or an accredited CA specifies an identity re-validation period, the expiry date of the certificate issued following re-key should not exceed the date on which identity re-validation for the previous certificate would be required unless the identity re-validation process followed. |
| 4.7.2 Who May Request Certification of a New Public Key | 3.2 Routine Re-key<br><br>4.1 Certificate Application | The scheme should record in its CP or other relevant documentation the classes of persons or organisations that can apply for certificate re-key. A CA accredited under the scheme may elect to accept applications from only some of these classes, in which case those classes should be recorded in the CP of the CA.<br><br>An RA accredited under the scheme may accept certificate re-key applications on behalf of a CA accredited under the scheme.<br><br>The scheme should allow a subscriber to make applications in respect of multiple subjects where a relationship between the subscriber and subject permitting such action is evidenced. |
| 4.7.3 Processing Certificate Re-Keying Requests | 3.2 Routine Re-key<br><br>4.1 Certificate Application<br><br>4.2 Certificate Issuance | The scheme should record in its CP or other relevant documentation the minimum processes to be followed for handling of applications for certificate re-key under the scheme.<br><br>The scheme may permit subscribers to apply for a certificate renewal using their current valid key pair.<br><br>A new certificate containing the new public key and same subject information as the previous certificate is issued and the existing certificate may be revoked.<br><br>Where the certificate or key pair usage period has expired the initial identification process should be followed. |
| 4.7.4 Notification of New Certificate Issuance to Subscriber | 3.2 Routine Re-key<br><br>4.2 Certificate Issuance<br><br>4.3 Certificate Acceptance | The scheme should record the minimum requirements for notification of new certificate issuance in its CP or other relevant documentation.<br><br>Notification may be by delivery of the certificate to the subscriber or subject accompanied by a statement of issue or by notification of the issuance of the certificate and the process for obtaining the certificate.<br><br>The scheme should permit electronic issue of new certificates following certificate renewal.<br><br>The scheme should record minimum requirements for verification of receipt of a new certificate and subsequent |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | publication of that certificate. These procedures may in part be met by a subscriber agreement that may have been signed at the time of application for certificate renewal. |
| 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate | 2.1.3 Subscriber Obligations<br><br>3.2 Routine Re-key<br><br>4.3 Certificate Acceptance | New certificate acceptance may be evidenced by formal acceptance or by use of the new certificate in accordance with the scheme.<br><br>Where the new certificate is not accepted within a specified time frame, or is rejected by the subscriber or subject, it should be immediately revoked. |
| 4.7.6 Publication of the Re-Keyed Certificate by the CA | 2.1.5 Repository Obligations<br><br>2.6.1 Publication of CA Information<br><br>3.2 Routine Re-key<br><br>4.3 Certificate Acceptance | New certificates should be published through a repository accredited under the scheme. The publication procedures should be recorded in the CA's CP and CPS. If the Repository operates as a separate entity, its responsibilities should also be recorded in the documentation of the Repository. The CA and the scheme should record their responsibilities for the operations of the Repository. |
| 4.7.7 Notification of Certificates Issuance by the CA to Other Entities | 2.1.5 Repository Obligations<br><br>2.6.1 Publication of CA Information<br><br>3.2 Routine Re-key<br><br>4.2 Certificate Issuance<br><br>4.3 Certificate Acceptance | A CA may notify other entities of new certificate issuance by direct notification or publication in a repository accessible by the other entity.<br><br>Where an RA processes certificate re-key applications on behalf of a CA, the CA should be notified of issuance and acceptance of that new certificate.<br><br>An accredited CA may publish its new certificate in addition to any publication or dissemination by the scheme itself.<br><br>A CA may publish any new certificates relating to its accreditation or any cross certificates with other CAs subject to the rules of the scheme. |
| 4.8 Certificate Modification | 4.4 Certificate Suspension and Revocation | A scheme may permit subscribers to apply for a certificate modification provided it does not affect the integrity of the scheme. Where modification changes subscriber or subject information, the changed information should be verified before new certificates are issued.<br><br>Where a change in subscriber information, such as organisational name, does not affect subject information on certificates issued to the subscriber, subject information may not need to be re-verified.<br><br>Where a scheme or an accredited CA specifies an identity re-validation period, the expiry date of the certificate issued following modification should not exceed the date on which identity re-validation for the previous certificate would be required unless the identity re-validation process followed.<br><br>Where the certificate or key pair has expired the initial identification process should be followed.<br><br>The scheme should not permit the modification of CSP certificates. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | NOTE: In cases of minor changes to subject information not impacting on relying parties, revocation of the existing certificate and issue of a new certificate may not be necessary. |
| 4.8.1 Circumstances for Certificate Modification | 2.1.3 Subscriber Obligations<br><br>4.4.1 Circumstances for Revocation | The Scheme should specify in its CP or other relevant documentation the types of information contained in a certificate that may be modified, the circumstances in which the data can be modified and the verification process required for such modification. For example a change of subscriber or subject name may be verified by sighting the name change documentation without the need to follow the full initial identification processes. Certificate modification is evidenced by the issue of a new certificate and revocation of the existing certificate.<br><br>Where the certificate or key pair has expired the initial identification process should be followed.<br><br>NOTE: In cases of minor changes to subject information not impacting on relying parties, revocation of the existing certificate and issue of a new certificate may not be necessary. |
| 4.8.2 Who May Request Certificate Modification | 4.4.2 Who Can Request Revocation | The scheme should record in its CP or other relevant documentation the classes of persons or organisations that can apply for certificate modification. A CA accredited under the scheme may elect to accept applications from only some of these classes, in which case those classes should be recorded in the CP of the CA.<br><br>An RA accredited under the scheme may accept certificate modification applications on behalf of a CA accredited under the scheme.<br><br>The scheme should allow a subscriber to make applications in respect of multiple subjects where a relationship between the subscriber and subject permitting such action is evidenced. |
| 4.8.3 Processing Certificate Modification Requests | 4.4.3 Procedure for Revocation Request | The scheme should record in its CP or other relevant documentation the minimum processes to be followed for handling of applications for certificate modification under the scheme.<br><br>A new certificate containing the same subject public key as the previous certificate and modified information is issued and the existing certificate revoked.<br><br>Where a scheme or an accredited CA specifies an identity re-validation period, the expiry date of the certificate issued following certificate modification should not exceed the date on which identity re-validation for the previous certificate would be required unless the identity re-validation process followed.<br><br>NOTE: In cases of minor changes to subject information not impacting on relying parties, revocation of the existing |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | certificate and issue of a new certificate may not be necessary. |
| 4.8.4 Notification of New Certificate Issuance to Subscribers | 4.2 Certificate Issuance<br><br>4.3 Certificate Acceptance<br><br>4.4.3 Procedure for Revocation Request | The scheme should record the minimum requirements for notification of new certificate issuance in its CP or other relevant documentation.<br><br>Notification may be by delivery of the new certificate to the subscriber or subject or by notification of the issuance of the new certificate and the process for obtaining the certificate.<br><br>The scheme should permit electronic issue of new certificates following certificate renewal.<br><br>The scheme should record minimum requirements for verification of receipt of a new certificate and subsequent publication of that certificate. These procedures may in part be met by a subscriber agreement that may have been signed at the time of application for certificate renewal. |
| 4.8.5 Conduct Constituting Acceptance of Modified Certificate | 2.1.3 Subscriber Obligations<br><br>4.3 Certificate Acceptance<br><br>4.4.3 Procedure for Revocation Request | New certificate acceptance may be evidenced by formal acceptance or by use of the new certificate in accordance with the scheme.<br><br>Where the new certificate is not accepted within a specified time frame, or is rejected by the subscriber or subject, it should be immediately revoked. |
| 4.8.6 Publication of the modified Certificate by the CA | 2.1.5 Repository Obligations<br><br>2.6.1 Publication of CA Information<br><br>4.2 Certificate Issuance<br><br>4.2 Certificate Acceptance<br><br>4.4.3 Procedure for Revocation Request | New certificates should be published through a repository accredited under the scheme. The publication procedures should be recorded in the CA CP and CPS. If the Repository operates as a separate entity, its responsibilities should also be recorded in the documentation of the Repository. The CA and the scheme should record their responsibilities for the operations of the Repository. |
| 4.8.7 Notification of Certificate Issuance by the CA to Other Entities | 2.1.5 Repository Obligations<br><br>2.6.1 Publication of CA Information<br><br>4.2 Certificate Issuance<br><br>4.2 Certificate Acceptance<br><br>4.4.3 Procedure for Revocation Request | A CA may notify other entities of new certificate issuance by direct notification or publication in a repository accessible by the other entity.<br><br>Where an RA processes certificate renewal applications on behalf of a CA, the CA should be notified of issuance and acceptance of that new certificate. |
| 4.9 Certificate Revocation and Suspension | 4.4 Certificate Suspension and Revocation | |
| 4.9.1 Circumstances for Revocation | 2.1.3 Subscriber Obligations | The scheme should set out the minimum circumstances |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | 4.4.1 Circumstances for Revocation | under which a subject certificate is to be revoked and the procedures for notification of revocation.<br><br>Where a scheme issues certificates to CAs accredited under the scheme, the circumstances under which those certificates will be revoked should also be set out.<br><br>As a minimum a subject's certificate should be revoked:<br><br>• Where a subject's private key has or may have been compromised;<br>• Where a subscriber ceases to be a member of the community of interest of, or withdraws from, the scheme;<br>• Where a subscriber or subject fails to meet their obligations under the scheme; or<br>• Where the information contained in a certificate is no longer correct.<br><br>NOTE: In cases of minor changes to subject information not impacting on relying parties, revocation of the existing certificate and issue of a new certificate may not be necessary.<br><br>A subject or CA certificate may be revoked:<br><br>• Where a certificate has been renewed; or<br>• Where a certificate has been re-keyed.<br><br>NOTE: Consideration should be given to potential requirements for a key roll-over period when revoking certificates following re-key.<br><br>As a minimum an accredited CA's certificate relating to the scheme should be revoked:<br><br>• Where a CA's private key has or may have been compromised.<br><br>• Where a CA ceases to be a member of the scheme; or<br><br>• Where a CA fails to meet their obligations under the scheme.<br><br>Where a CA's certificate is revoked the scheme should record the procedures for the reissue of subject certificates issued by that CA. |
| 4.9.2 Who Can Request Revocation | 4.4.2 Who Can Request Revocation | Where a scheme issues certificates to CAs it should have the power to revoke that certificate at the request of itself or the CA named in the certificate.<br><br>The scheme should set out the parties who can request revocation of a subscriber certificate and the circumstances in which they can make such a request. This does not prevent a CA accredited under the scheme from allowing additional revocation criteria provided they are published. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | As a minimum a subscriber, subject named in a certificate or the CA issuing the certificate should be allowed to request revocation in the case of an actual or suspected compromise of the subject's private key.<br><br>The scheme, a CA, RA, or subscriber should be permitted to revoke a certificate where a subject leaves the community of interest covered by the scheme or that CA, RA or subscriber.<br><br>The scheme, a CA, RA or subscriber should be allowed to revoke the certificate of a subscriber or subject who fails to meet their obligations to the scheme, or to that CA, RA or subscriber.<br><br>The subscriber, RA or CA should be allowed to revoke a certificate where the subject information contained in the certificate has changed. |
| 4.9.3 Procedure for Revocation Request | 2.1.3 Subscriber Obligations<br><br>4.4.3 Procedure for Revocation Request | The scheme should record the procedure for processing requests for revocation of certificates of CAs accredited under the scheme and subscribers.<br><br>Where a request to revoke the certificate of an accredited CA is received by a scheme it should record the person making the request, reason for the request, steps taken to verify the request, time and date of revocation and notification of revocation to the CA, its subscribers and relying parties.<br><br>Where a CA receives a request to revoke a subject certificate it should record the person making the request, relationship with the subject, reason for the request, steps taken to verify the request, time and date of revocation and notification of revocation to the CA, its subscribers and relying parties. If a request for revocation is not accepted the reasons for that action should also be recorded.<br><br>A subscriber's responsibilities for requesting revocation of their certificates should be recorded in the subscriber agreement. |
| 4.9.4 Revocation Request Grace Period | 4.4.4 Revocation Request Grace Period | The scheme should record any grace period following an event requiring revocation within which the person requesting revocation should make or confirm a revocation request<br><br>As a general rule any grace period granted should not exceed the frequency of publication of CRLs. |
| 4.9.5 Time Within Which CA Must Process the Revocation Request | No Provision | A revocation request should be processed within 24 hours of the expiry of any revocation request grace period.<br><br>NOTE: For CAs including scheme CAs, who only issue certificates to subordinate, cross recognised or cross certified CAs, security procedures, off-line nature and physical separation from the repository may require a longer period. In these cases the CRL should be posted as soon as practicable. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 4.9.6 Revocation Checking Requirements for Relying Parties | 2.1.4 Relying Party Obligations<br><br>4.4.10 CRL Checking Requirements<br><br>4.4.12 On-line Revocation Checking Requirements<br><br>4.4.14 Checking Requirements for Other Forms of Revocation Advertisements | The scheme should ensure that potential relying parties are aware of their obligations to establish the validity of a certificate at the time of the transaction and of the consequences of failure to do so. Notification can be by way of a PKI disclosure statement or similar document published or made accessible to the relying party.<br><br>Where a scheme is likely to publish revocation information through media advertisements it should advise subscribers and potential relying parties of the form of publication and the implications of that form of publication. |
| 4.9.7 CRL Issuance Frequency | 4.4.9 CRL Issuance Frequency (if applicable)<br><br>4.8.3 Entity key is Compromised | Where a scheme revokes the certificate or changes the status of a CA accredited under the scheme, or cross recognised or cross certified by the scheme, the change shall be notified immediately. Such notification should include any other schemes that recognise the scheme.<br><br>The scheme should set out the CRL issuance or certificate status update frequency. As a minimum this should be not less than once every 24 hours. This provision does not apply for CAs, including scheme CAs, who only issue certificates to subordinate, cross recognised or cross certified CAs.<br><br>CRLs should comply with the provisions of X.509. Delta CRLs and CRL Distribution Points may be supported.<br><br>Where a scheme or CA accredited under a scheme revokes its public key the situation should be notified through the immediate issue of a CRL or an update of status information. The notification should include all other schemes that recognise certificates issued by the scheme. For a CA accredited under the scheme the notification should be signed by the scheme, where possible.<br><br>Following revocation a new key should be generated and notified.<br><br>Where a scheme does not issue certificates or where it is the scheme public key that is revoked, any notification of revocation should provide a mechanism for confirmation of the revocation through a separate channel to the notification. |
| 4.9.8 Maximum Latency for CRLs | 4.4.9 CRL Issuance Frequency (if applicable) | The scheme should set out the maximum latency between generation of CRLs and their posting to the repository. This should be not more than one hour from generation of the CRL. Delta CRLs and CRL Distribution Points may be supported.<br><br>NOTE: For CAs including scheme CAs, who only issue certificates to subordinate, cross recognised or cross certified CAs, security procedures, off-line nature and physical separation from the repository may require a longer period. In these cases the CRL should be posted as soon as practicable. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 4.9.9 On-Line Revocation/Status Checking Availability | 4.4.11 On-line Revocation/Status Checking Availability<br><br>4.8.3 Entity Key is Compromised | Where on-line revocation/status checking is supported it should be available with the same reliability as any CRL or directory it replaces or operates in conjunction with.<br><br>Where a scheme or CA accredited under a scheme revokes its public key the situation should be notified through the immediate issue of a CRL or an update of status information. The notification should include all other schemes that recognise certificates issued by the scheme. For a CA accredited under the scheme the notification should be signed by the scheme, where possible.<br><br>Following revocation a new key should be generated and notified.<br><br>Where a scheme does not issue certificates or where it is the scheme public key that is revoked, any notification of revocation should provide a mechanism for confirmation of the revocation through a separate channel to the notification. |
| 4.9.10 On-Line Revocation Checking Requirements | 4.4.12 On-line Revocation Checking Requirements | The scheme should ensure that potential relying parties are aware of their obligations to establish the validity of a certificate at the time of the transaction and of the consequences of failure to do so. Notification can be by way of a PKI disclosure statement or similar document published or made accessible to the relying party. |
| 4.9.11 Other Forms of Revocation Advertisements Available | 4.4.13 Other Forms of Revocation Advertisements Available<br><br>4.4.14 Checking Requirements for Other Forms of Revocation Advertisements<br><br>4.8.3 Entity Key is Compromised | A scheme should permit either itself, an affected CA or subscriber to use other forms of advertisement of revocation where such advertising may reduce the risk to potential relying parties.<br><br>Where a scheme has revoked its own certificate or revoked the certificate or changed the status of an accredited CA it should consider advertising that fact together with guidance to subscribers and potential relying parties on action to be taken. Advertising may extend to other jurisdictions that recognise the scheme.<br><br>Where a scheme is likely to use advertising it should advise subscribers and potential relying parties of the form of advertising and the implications of that advertising.<br><br>Where a scheme or CA accredited under a scheme revokes its public key the situation should be notified through the immediate issue of a CRL or an update of status information. The notification should include all other schemes that recognise certificates issued by the scheme. For a CA accredited under the scheme the notification should be signed by the scheme, where possible. |
| 4.9.12 Special Requirements re Key Compromise | 4.4.15 Special Requirements re Key Compromise | The scheme should record any special requirements regarding key compromise in its CP or other relevant documentation. |
| 4.9.13 Circumstances for Suspension | 2.1.3 Subscriber Obligations<br><br>4.4.5 Circumstances for | Where a scheme permits the suspension of subject certificates the circumstances and procedures for such suspension and notification of the suspension should be |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | Suspension | recorded.<br><br>Subscriber and subject responsibilities for requesting suspension should be recorded in the subscriber agreement.<br><br>Where legislation places certain obligations on subscribers or subjects to ensure the legal effect of transactions utilising certificates issued by the CA the subscriber agreement should record those obligations.<br><br>Where a jurisdiction places obligations on subscribers to, or subjects of, schemes outside that jurisdiction those obligations should be made available to those subscribers and subjects. |
| 4.9.14 Who can Request Suspension | 4.4.6 Who can Request Suspension | Where suspension is permitted under the scheme the same persons that can request revocation may be permitted to request suspension. |
| 4.9.15 Procedure for Suspension Request | 2.1.3 Subscriber Obligations<br><br>4.4.7 Procedure for Suspension Request | Procedures for processing a suspension should be similar to those for a request for revocation. In addition the procedures should record whether the certificate was ultimately revoked or not and the reasons for that decision. |
| 4.9.16 Limits on Suspension Period | 4.4.8 Limits on Suspension Period | The scheme should indicate the limit on any suspension period. In any event it should not exceed one month from the time the request was received. |
| 4.10 Certificate Status Services | 4.4.9 CRL Issuance Frequency (if applicable)<br><br>4.4.10 CRL Checking Requirements<br><br>4.4.11 On-line Revocation/Status Checking Availability<br><br>4.4.12 On-line Revocation Checking Requirements<br><br>4.4.13 Other Forms of Revocation Advertisements Available<br><br>4.4.14 Checking Requirements for Other Forms of Revocation advertisements | The scheme should record in its CP or other relevant documentation whether certificate status service, including OCSP, validation authorities, certificate trust lists and trust status information are supported by the scheme. |
| 4.10.1 Operational Characteristics | 4.4.9 CRL Issuance Frequency (if applicable)<br><br>4.4.11 On-line Revocation/Status Checking Availability<br><br>4.4.13 Other Forms of | The scheme should specify the operational characteristics of any certificate status services supported by the scheme.<br><br>Any certificate status information should be digitally signed and time and date stamped by the entity generating that information. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | Revocation Advertisements Available | |
| 4.10.2 Service Availability | 4.4.9 CRL Issuance Frequency (if applicable)<br><br>4.4.11 On-line Revocation/Status Checking Availability<br><br>4.4.13 Other Forms of Revocation Advertisements Available | Where certificate status information is supported it should be available with the same reliability as any CRL or directory it replaces or operates in conjunction with. |
| 4.10.3 Operational Features | 4.4.9 CRL Issuance Frequency (if applicable)<br><br>4.4.11 On-line Revocation/Status Checking Availability<br><br>4.4.13 Other Forms of Revocation Advertisements Available | The scheme should record in its CP or other relevant documentation any optional features or value added services of certificate status services that are permitted or supported by the scheme. |
| 4.11 End of Subscription | No Provision | The scheme should record in its CP or other relevant documentation the procedures used by subscribers to end subscription to the scheme. This should include any on-going scheme, CA and subscriber responsibilities arising from the subscriber's participation in the scheme.<br><br>Subscriber responsibilities at the end of subscription should be recorded in the subscriber agreement.<br><br>Where legislation places certain obligations on subscribers or subjects to ensure the legal effect of transactions utilising certificates issued by the CA the subscriber agreement should record those obligations.<br><br>Where a jurisdiction places obligations on subscribers to, or subjects of, schemes outside that jurisdiction those obligations should be made available to those subscribers or subjects.<br><br>Where a subscriber elects to end subscription to the scheme, or the CA terminates the subscriber's subscription, the subscriber's certificate, and the certificates of any subjects enrolled by the subscriber should be revoked. |
| 4.12 Key Escrow and Recovery | 6.2.3 Private Key Escrow | Escrow of private signing keys should not be supported.<br><br>Escrow of private encryption keys should only be permitted with the consent of the subscriber.<br><br>NOTE: Some jurisdictions that have implemented the OECD Guidelines for Cryptography Policy require the use of separate encryption and signing keys to allow law enforcement access to encryption keys without |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | compromising signing keys. This issue may need to be addressed in cross recognition agreements.<br><br>NOTE 2: Some schemes may support separate keys and CPs for encryption and signing. Where a separate CP supports signing keys only, only para 1 of 4.12 will apply." |
| 4.12.1 Key Escrow and Recovery Policy and Practices | 6.2.3 Private Key Escrow | Where escrow of private encryption keys is supported, the scheme should record in its CP or other relevant documentation its policy and practices in respect of the escrow and recovery. This should include arrangements for securing the keys, persons permitted to access the keys and the processes for access and notification of access.<br><br>Where escrow of private encryption keys in supported, consent for authorised access should be offered in the subscriber agreement.<br><br>Where legislation places certain obligations on subscribers or subjects to provide access to private encryption keys the subscriber agreement should record those obligations.<br><br>Where a jurisdiction places obligations on subscribers to, or subjects of, schemes outside that jurisdiction those obligations should be made available to those subscribers or subjects.<br><br>NOTE: Some jurisdictions that have implemented the OECD Guidelines for Cryptography Policy require the use of separate encryption and signing keys to allow law enforcement access to encryption keys without compromising signing keys. This issue may need to be addressed in cross recognition agreements.<br><br>NOTE 2: Some schemes may support separate keys and CPs for encryption and signing. Where a separate CP supports signing keys only, only para 1 of 4.12 will apply." |
| 4.12.2 Session Key Encapsulation and Recovery Policy and Practices | 6.2.3 Private Key Escrow | Session keys are used for encryption only and are generally outside the scope of these guidelines unless the recovery process involves escrow of, or access to, a private key that may also be used for signing.<br><br>Where a scheme permits an accredited CA to be directly involved in session key encapsulation using a technique that involves escrow of a subject private key associated with a public key certified by the CA, the provisions of 4.12.1 would apply.<br><br>Where a subscriber undertakes session key encapsulation for the transactions of subjects enrolled by the subscriber, such action is outside the scope of these guidelines. However any subscriber obligations to protect subject private keys that may be used in the encapsulation process would still apply. |
| 5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS | 2.1.3 Subscriber Obligations<br><br>2.1.4 Relying Party | ISO/IEC 17799 "Information technology – Code of practice for information security management" and ISO/IEC TR13335 "Information technology -- Guidelines for the management of IT Security" can provide guidance on the |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | Obligations<br><br>4. OPERATIONAL REQUIREMENTS<br><br>5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS | types of controls that should be implemented.<br><br>Where a scheme or legislation places certain non-technical security responsibilities on subscribers or subjects, these should be recorded or referenced in the subscriber agreement.<br><br>Where a scheme or legislation places certain non-technical security responsibilities on relying parties, these should be recorded or referenced a PKI disclosure statement or similar document published and made accessible to the relying party. |
| 5.1 Physical Controls | 5.1 Physical Controls | The scheme should record in its CP or other relevant documentation the physical security measures that are to be implemented for the scheme facilities, equipment and data and for CSPs accredited under the scheme. |
| 5.1.1 Site Location and Construction | 5.1.1 Site Location and Construction | The site location and construction should be to a standard appropriate for the protection of the collective value of the assets or transactions protected by the scheme.<br><br>Public access areas such as registration offices should be separated from areas housing the records and equipment for the operation of the CSP activity covered by the scheme. |
| 5.1.2 Physical Access | 5.1.2 Physical Access | Physical access to facilities should be monitored and controlled.<br><br>In addition access to non public areas should be logged.<br><br>Visitors, including contractors and maintenance staff, should have their identity verified before access to non public areas is granted. Consideration should be given to background checks for visitors where their access to scheme facilities and systems warrants such checks. Visitors should be identified as such and escorted where appropriate. |
| 5.1.3 Power and Air Conditioning | 5.1.3 Power and Air Conditioning | Power and air conditioning equipment, including backup equipment, should be protected and maintained to ensure operations meet their availability requirements under the scheme |
| 5.1.4 Water Exposures | 5.1.4 Water Exposures | The facility should be protected against water exposure. |
| 5.1.5 Fire Prevention and Protection | 5.1.5 Fire Prevention and Protection | The facility should have adequate fire prevention and protection facilities. |
| 5.1.6 Media Storage | 5.1.6 Media Storage | Both electronic and paper records and media should be protected against unauthorised access and deliberate or accidental damage or destruction including damage by fire, temperature, water, humidity and magnetism. |
| 5.1.7 Waste Disposal | 5.1.7 Waste Disposal | All electronic and paper waste, including media, shall be securely destroyed or erased and sanitised. |
| 5.1.8 Off-Site Backup | 5.1.8 Off-site Backup | Off site backup records and facilities should be established and maintained consistent with the archives policy and business continuity and disaster recovery plans. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 5.2 Procedural Controls | 5.2 Procedural Controls | The scheme should record in its CP or other relevant documentation the procedural security measures that are to be implemented for the scheme facilities, equipment and data and for CSPs accredited under the scheme. |
| 5.2.1 Trusted Roles | 5.2.1 Trusted Roles | The scheme should define what are considered to be trusted roles in the operation of the scheme and of CSPs accredited under the scheme.<br><br>The description of the roles should include the tasks that can and cannot be undertaken by those filling the roles and should be provided to those undertaking the roles. Written acknowledgment should be obtained. |
| 5.2.2 Number of Persons Required per Task | 5.2.2 Number of Persons Required per Task | The scheme should identify tasks that require more than one person to perform the task.<br><br>As a minimum, generation of scheme or CA signing keys should require more than one person to perform the task. Consideration should be given to requiring more than one person for tasks involving access to cryptographic modules containing the scheme or CA signing keys. |
| 5.2.3 Identification and Authentication for Each Role | 5.2.3 Identification and Authentication for Each Role | Physical and logical access controls should verify identity and authorisation before access is granted. |
| 5.2.4 Roles Requiring Separation of Duties. | 5.2.1 Trusted Roles<br><br>5.2.2 Number of Persons Required per Task | The scheme should define what are considered to be roles requiring separation of duties in the operation of the scheme and of CSPs accredited under the scheme.<br><br>As a minimum, persons implementing a function should not also have the role of compliance audit, assessment or review of that implementation. Other areas of potential conflict may also be identified. |
| 5.3 Personnel Controls | 5.3 Personnel Controls | The scheme should record in its CP or other relevant documentation the personnel security measures that are to be implemented for the scheme personnel and those of CSPs accredited under the scheme.<br><br>The scheme should set out in its CP or other relevant documentation any secrecy, confidentiality and non disclosure provisions in legislation governing the scheme, legislation governing transactions utilising the scheme, legislation governing employees participating in the scheme and any other relevant legislation such as privacy legislation. This information should be provided in writing to employees and contractors under the scheme, CSPs accredited under the scheme and their employees and a written acknowledgment obtained.<br><br>This information should be incorporated in any contracts for employment or services. |
| 5.3.1 Qualifications, Experience, and Clearance Requirements | 5.3.1 Background, Qualifications, Experience, and Clearance Requirements | The scheme should document in its CP or other relevant documentation the qualifications, experience and clearance requirements for its personnel and contractors and those of any CSP accredited under the scheme. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 5.3.2 Background Check Procedures | 5.3.2 Background Check Procedures | The scheme should set out the background check procedures and may nominate who is to carry out those checks.<br><br>Personnel filling trusted roles should be cleared to a level consistent with the sensitivity or collective value of the assets and transactions protected by the activity for which they are responsible.<br><br>In general this will involve verification of identity, qualifications and references; checks for criminal convictions; and credit or similar financial checks within the requirements of any privacy and spent convictions legislation that might apply. |
| 5.3.3 Training Requirements | 5.3.3 Training Requirements | The scheme should set out in its CP or other relevant documentation the training requirements for its personnel and contractors and those of CSPs accredited under the scheme.<br><br>As a minimum this should include:<br><br>• The equipment and software they are required to operate<br><br>• The aspects of the CP, CPS, security policy and other relevant documentation affecting their duties<br><br>• Legislative requirements covering their duties<br><br>• Their roles under business continuity and disaster recovery plans |
| 5.3.4 Retraining Frequency and Requirements | 5.3.4 Retraining Frequency and Requirements | As a minimum retraining should be undertaken whenever there are significant changes in the elements contained in the initial training. |
| 5.3.5 Job Rotation Frequency and Sequence | 5.3.5 Job Rotation Frequency and Sequence | The scheme and any CSP accredited under the scheme should record in their CP or other relevant documentation any job rotation policies. For some government operated schemes and CSPs government job rotation policies may apply.<br><br>Where job rotation does apply, job handover procedures should be documented including minimum handover periods. |
| 5.3.6 Sanctions for Unauthorized Actions | 5.3.6 Sanctions for Unauthorized Actions | The scheme should record in its CP or other relevant documentation the sanctions for unauthorised actions.<br><br>As a minimum in the event of an actual or suspected unauthorised action by a person filling a trusted role, that person should be immediately suspended from that or any other trusted role. |
| 5.3.7 Contracting Personnel Requirements | 5.3.7 Contracting Personnel Requirements | The scheme should set out in its CP or other relevant documentation whether contractors are permitted to be used.<br><br>The scheme should require contractors and their staff to be subject to the same personnel controls as employees under |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | the scheme. This should be reflected in any contracts.<br><br>Contactors and their staff should be bound by the CP, CPS and other relevant documentation of the scheme, CSP with whom they contract.<br><br>Contracts should specify sanctions and damages provisions for actions by the contractor and its employees. |
| 5.3.8 Documentation Supplied to Personnel | 5.3.8 Documentation Supplied to Personnel | Personnel should be provided with the documentation necessary to carry out their duties.<br><br>As a minimum this should include:<br><br>• A statement of duties and authorisations.<br><br>• Manuals for the equipment and software they are required to operate<br><br>• The aspects of the CP, CPS , security policy and other relevant documentation affecting their duties<br><br>• Legislation covering their duties<br><br>• Documentation of their roles under business continuity and disaster recovery plans |
| 5.4 Audit Logging Procedures | 4.5 Security Audit Procedures | The scheme should record in its CP or other relevant documentation the minimum audit log requirements for itself and any CSPs accredited under the scheme. |
| 5.4.1 Types of Event Recorded | 4.5.1 Types of Event Recorded | The scheme should ensure that CSPs maintain audit logs of events that are likely to impact the security and operation of the scheme.<br><br>As a minimum these should include actual or attempted access and/or modification of key applications; actual or attempted actions in respect of keys, certificates, subscriber records; changes in system configuration; and system availability.<br><br>Physical access to secure areas should be recorded.<br><br>Audit log events should record time, date and any software/hardware identifiers. |
| 5.4.2 Frequency of Processing Log | 4.5.2 Frequency of Processing Log | The scheme should record in its CP or other relevant documentation the frequency with which audit logs should be processed.<br><br>As a minimum audit logs should be processed and the results reviewed on a weekly basis.<br><br>Significant auditable events should generate automated alarms. |
| 5.4.3 Retention Period for Audit Log | 4.5.3 Retention Period for Audit Log | The scheme should record in its CP or other relevant documentation the period for retention of audit logs.<br><br>As a minimum audit logs should be retained for a period of |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | seven years or the maximum period required by any jurisdiction with which the scheme has a cross recognition agreement. |
| 5.4.4 Protection of Audit Log | 4.5.4 Protection of Audit Log | The scheme should record in its CP or other relevant documentation its requirements for the protection of audit logs from unauthorised access, modification or deletion. |
| 5.4.5 Audit Log Backup Procedures | 4.5.5 Audit Log Backup Procedures | The scheme should record in its CP or other relevant documentation audit log backup procedures.<br><br>As a minimum audit logs should be backed up monthly and a copy stored off site.<br><br>Consideration should be given to automated backup of significant auditable events. |
| 5.4.6 Audit collection system (Internal vs External) | 4.5.6 Audit Collection System (Internal vs External) | The scheme should record in its CP or other relevant documentation whether audit logs should be collected internally, externally or whether accredited CSPs can elect which approach to use.<br><br>Audit log collection should be undertaken while ever the system is operational. |
| 5.4.7 Notification to Event-causing Subject | 4.5.7 Notification to Event-causing Subject | The scheme should record in its CP or other relevant documentation whether an event-causing subject can be notified.<br><br>Consideration should be given to allowing a subject to be notified where the event is established to be accidental and likely to re-occur. |
| 5.4.8 Vulnerability Assessments | 4.5.8 Vulnerability Assessments | The scheme should record in its CP or other relevant documentation whether vulnerability assessment of systems is required and if so with what frequency.<br><br>A distinction may need to be made between vulnerability assessment (passive assessment of potential vulnerabilities) and vulnerability testing (active attempts to penetrate systems to identify vulnerabilities). |
| 5.5 Records Archival | 4.6 Records Archival | The scheme should record in its CP or other relevant documentation the records the scheme will archive and the period of retention.<br><br>The scheme should record in its CP or other relevant documentation the records CSPs are required to archive and the period of retention. |
| 5.5.1 Types of Event Recorded | 4.6.1 Types of Event Recorded | The scheme should require the archiving of any information required to establish the validity of a certificate for the period that records must be retained in any jurisdiction with which the scheme has a cross recognition agreement. This should include scheme records and records of CSPs accredited under the scheme.<br><br>As a minimum subscriber information; certificate databases; revocation or status information; scheme, CA and RA public |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | keys; and audit logs should be retained. |
| 5.5.2 Retention Period for Archive | 4.6.2 Retention Period for Archive | The scheme should record in its CP or other relevant documentation the period for retention of archives.<br><br>As a minimum archives should be retained for a period of seven years or the maximum period required by any jurisdiction with which the scheme has a cross recognition agreement.<br><br>Applications required to access an archive should also be archived. |
| 5.5.3 Protection of Archive | 4.6.3 Protection of Archive | The scheme should record in its CP or other relevant documentation the measures required to protect archived information.<br><br>As a minimum the measures should prevent any modification or deletion of data contained in the archive.<br><br>Consideration may be given to re-signing archives where advances in technology have the potential to compromise the archive. |
| 5.5.4 Archive Backup Procedures | 4.6.4 Archive Backup Procedures | The scheme should record the requirements for backup of archives generated by the scheme and CSPs accredited under the scheme. |
| 5.5.5 Requirements for Time-stamping of Records | 4.6.5 Requirements for Time-stamping of Records | Archive data should be time and date stamped and digitally signed by the organisation generating the archive or protected in some other way that can demonstrate it originates from the organisation generating the archive. |
| 5.5.6 Archive Collection System (Internal or External) | 4.6.6 Archive Collection System (Internal or External) | The scheme should require that at least two backups are retained, one of which to be held off site. |
| 5.5.7 Procedures to Obtain and Verify Archive Information | 4.6.7 Procedures to Obtain and Verify Archive Information | The scheme should record in its CP or CPS the procedures to obtain and verify archive information.<br><br>The procedures should be consistent with the confidentiality and privacy requirements detailed under 9.3 and 9.4. |
| 5.6 Key Changeover | 4.7 Key Changeover | The scheme should record in its CP or other relevant documentation the policy regarding key changeover for the scheme, where applicable, CAs accredited under the scheme and subscribers.<br><br>The scheme may permit automatic key changeover during the period of validity of the current key.<br><br>The scheme should only permit scheme and CA key changeover where keys used to sign valid certificates issued by the scheme or CA are retained until those certificates have expired. |
| 5.7 Compromise and Disaster Recovery | 4.8 Compromise and Disaster Recovery | The scheme should ensure that business continuity and disaster recovery plans for the scheme and CSPs accredited under the scheme are established and maintained.<br><br>The plans should ensure that basic business such as |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | certificate validation and revocation services can be resumed within 24 hours which is the maximum period for the issue of certificate revocation lists.<br><br>The plans should be tested at least once during each compliance audit or assessment period and the results made available to the compliance auditors or assessors together within information on any remedial action taken.<br><br>NOTE: For CAs including scheme CAs, who only issue certificates to subordinate, cross recognised or cross certified CAs, security procedures and off-line nature may require a longer period. In these cases the certificate revocation and certificate re issue services should be resumed as soon as practicable. |
| 5.7.1 Incident and Compromise Handling Procedures | 4.8 Compromise and Disaster Recovery | Business continuity and disaster recovery plans should specifically address procedures to be followed in the event of an actual or suspected incident or compromise of the integrity of the scheme or CSP operations. |
| 5.7.2 Computing Resources, Software, and/or Data are Corrupted | 4.8.1 Computing Resources, Software, and/or Data are Corrupted | The plans should identify alternate sources of computing resources, software and data to be utilised in the event of corruption or failure.<br><br>Where corruption renders private keys suspect or inoperable consideration should be given to re-keying. |
| 5.7.3 Entity Private Key Compromise Procedures | 4.8.3 Entity Key is Compromised | Should the key of a scheme or CA accredited under the scheme be compromised or suspected of being compromised it should immediately be revoked and the notification procedures above followed. |
| 5.7.4 Business Continuity Capabilities After a Disaster | 4.8.4 Secure Facility After a Natural or Other Type of Disaster | The scheme should record requirements for operations of a facility where a natural or other disaster may affect the security of that facility.<br><br>Generally the scheme should require an organisation to operate from a secure alternate facility or use a secure backup copy of software and data until the secure operation of the prime facility can be assured. |
| 5.8 CA or RA Termination | 4.9 CA Termination | The scheme should require a CSP to give notice prior to termination or transfer of ownership or operations.<br><br>Where a CSP terminates its operations the scheme should ensure that all data necessary for continuation of scheme operations is transferred to a CSP nominated by the scheme or to the scheme itself. This may require the scheme acquiring licenses to ensure continuation of operations previously undertaken by the terminating CSP.<br><br>Where a transfer of ownership or operations is involved the scheme should ensure the new owners or operators achieve accreditation under the scheme. Where this is not practicable the scheme should consider taking over operations until the new owner or operator is accredited.<br><br>The scheme should advise all subscribers and relying parties |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | of the changes and any conditions associated with continued use of certificates issued by the terminating or transferring CSP. |
| 6. TECHNICAL SECURITY CONTROLS | 2.1.3 Subscriber Obligations<br><br>2.1.4 Relying Party Obligations<br><br>6. TECHNICAL SECURITY CONTROLS | ISO/IEC 17799 "Information technology – Code of practice for information security management" and ISO/IEC TR13335 "Information technology -- Guidelines for the management of IT Security" can provide guidance on the types of controls that should be implemented.<br><br>ISO/IEC 15408 "Information technology -- Security techniques -- Evaluation criteria for IT security" can be used to evaluate technology used in a PKI operation.<br><br>Where a scheme or legislation places certain technical security responsibilities on subscribers, subjects or relying parties, these should be recorded or referenced in the subscriber or relying party agreements. |
| 6.1 Key Pair Generation and Installation | 6.1 Key Pair Generation and Installation | The scheme should set out in its CP or other relevant documentation the procedures for key generation by the scheme, CAs accredited under the scheme and subscribers as applicable. |
| 6.1.1 Key Pair Generation | 6.1.1 Key Pair Generation<br><br>6.1.8 Hardware/Software Key Generation | Keys under the scheme should be generated using key generation processes approved by the scheme. Keys may be generated by subscribers or CAs.<br><br>Keys generated for use by the scheme or for use by CSPs accredited under the scheme should be generated by approved means.<br><br>Keys for use by subscribers or subjects may be generated in either approved hardware cryptographic modules or using approved software packages or processes.<br><br>Keys should be verified before a certificate is issued. |
| 6.1.2 Private Key Delivery to Subscriber | 6.1.2 Private Key Delivery to Entity | Where a CA or RA generates keys on behalf of a subscriber, controls should be implemented to ensure the secrecy of the associated private key.<br><br>Where the keys are not issued to the subscriber or subject in person, the scheme should permit electronic issue of keys provided separate trusted channels are used for issue of the key and an activation code (or activation codes) for the key. |
| 6.1.3 Public Key Delivery to Certificate Issuer | 6.1.3 Public Key Delivery to Certificate Issuer | Where a subscriber generates their own key pair or subject key pairs, the relevant public key/s should be delivered to the certificate issuer in a manner that ensures the authenticity of the subscriber.<br><br>Where RAs accept public keys on behalf of certificate issuers, they should be delivered to the certificate issuer in a way that ensures the association between the subject and key is maintained. |
| 6.1.4 CA Public Key delivery to Relying | 6.1.4 CA Public Key Delivery to Users | Where the scheme generates certificates it should publish the corresponding public key on a site accessible to potential |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| Parties | | relying parties.<br><br>Where the scheme is recognised by other schemes the key should be delivered to those schemes in a manner that ensures the authenticity and integrity of the key.<br><br>The public keys of CAs accredited under the scheme can be delivered through certificates signed by the scheme or can be retained in a directory of cross certificates or status information maintained by the scheme. |
| 6.1.5 Key Sizes | 6.1.5 Key Sizes | The scheme should set out in its CP or other relevant documentation the algorithms and key lengths used by the scheme.<br><br>As a minimum the scheme should support the used of RSA and DSA and SHA1. The use of ECDSA may be supported.<br><br>Any key pairs generated for the operation of the scheme or of CSPs accredited under the scheme should be a minimum of 2048 bit RSA or DSA.<br><br>Any key pairs generated for subscribers or subjects under the scheme should be a minimum of 1024 bit RSA or DSA.<br><br>NOTE: While some schemes may support different algorithms and key lengths domestically, they should ensure that the algorithms and key lengths outlined above are available and supported for external e-commerce transactions. They should also support and recognise certificates from external schemes that utilise these algorithms and minimum key lengths. Consideration should be given to supporting ECDSA as soon as possible |
| 6.1.6 Public Key Parameters Generation and Quality Checking | 6.1.6 Public Key Parameters Generation<br><br>6.1.7 Parameter Quality Checking | The scheme should assess the public key parameters to be used in the scheme and who can generate those parameters.<br><br>In general the parameters will be generated by an accredited CA or a trusted process nominated by the CA<br><br>The scheme should ensure that as a minimum compliance audit or assessment processes should check the quality of any parameters generated by a CA accredited under the scheme. |
| 6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) | 6.1.9 Key Usage Purposes (as per X.509 v3 Key Usage Field) | The scheme should recognise that signing keys can be distinguished from encrypting keys in the key usage field of the certificate for that key.<br><br>The CertSign and CRLSign bits should only be set for the scheme or CAs accredited under the scheme.<br><br>NOTE: Some jurisdictions that have implemented the OECD Guidelines for Cryptography Policy require the use of separate encryption and signing keys to allow law enforcement access to encryption keys without compromising signing keys. This issue may need to be addressed in cross recognition agreements. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 6.2 Private Key Protection and Cryptographic Module Engineering Controls | 6.2 Private Key Protection<br><br>6.8 Cryptographic Module Engineering Controls | The scheme should set out in its CP or other relevant documentation the requirements for private key protection for all keys generated under the scheme.<br><br>Proposed standard ISO/IEC 19790 based on FIPS 140-2 is being developed to address cryptographic module engineering controls.<br><br>NOTE: ISO/IEC 15408 based Protection Profiles for cryptographic devices certified EAL4+ are defined in: CWA 14169 (subjects' devices), CWA 14167-2 and –4 for CAs, TSAs, etc. signing, CWA 14167-3 for key generation outside the signing device<br><br>CEN Workshop Agreements (CWAs) 14169, 14167-2, 14167-3, 14167-4 are ISO 15408 - Common Criteria - compliant Protection Profiles for signing devices developed by a CEN (Comité Européen de Normalisation- www.cenorm.be) Workshop within the European Electronic Signature Specification Initiative. These documents can be accessed at URL http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/cwa/electronic+signatures.asp.<br><br>TSA: Time Stamping Authority: authority which issues time-stamp tokens (RFC 3628) |
| 6.2.1 Cryptographic Module Standards and Controls | 6.2.1 Standards for Cryptographic Modules<br><br>6.8 Cryptographic Module Engineering Controls | Cryptographic modules used by the scheme or CAs should meet the requirements of, or equivalent to, FIPS 140-1 level 3.<br><br>Cryptographic modules used by CSPs accredited under the scheme should meet the requirements of, or equivalent to, FIPS 140-1 level 2.<br><br>Cryptographic modules used by subjects under the scheme should meet the requirements of, or equivalent to, FIPS 140-1 level 1.<br><br>Proposed standard ISO/IEC 19790 based on FIPS 140-2 is being developed to address this requirement. |
| 6.2.2 Private Key (n out of m) Multi-person Control | 6.2.2 Private Key (n out of m) Multi-person Control | The scheme should ensure that the generation of, and access to, the private keys of the scheme or CSPs accredited under the scheme should require at least two persons acting in concert. |
| 6.2.3 Private Key Escrow | 6.2.3 Private Key Escrow | Escrow of private signing keys should not be supported.<br><br>Escrow of private encryption keys should only be permitted with the consent of the subscriber.<br><br>NOTE: Some jurisdictions that have implemented the OECD Guidelines for Cryptography Policy require the use of separate encryption and signing keys to allow law enforcement access to encryption keys without compromising signing keys. This issue may need to be addressed in cross recognition agreements. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 6.2.4 Private Key Backup | 6.2.4 Private Key Backup | Backup of the private keys of the scheme and of CSPs accredited under the scheme should be permitted provided the protection provided to the backup is not less than that provided for the master copy. |
| 6.2.5 Private Key Archival | 6.2.5 Private Key Archival | Private keys used only for signing should not be archived unless required under applicable law.<br><br>Other private keys may be archived to allow restoration of material as required.<br><br>Where private keys are archived they should be protected at the same level as an active key<br><br>NOTE: Some jurisdictions that have implemented the OECD Guidelines for Cryptography Policy require the use of separate encryption and signing keys to allow law enforcement access to encryption keys without compromising signing keys. This issue may need to be addressed in cross recognition agreements |
| 6.2.6 Private Key Transfer Into or From a Cryptographic Module | 6.2.6 Private Key Entry into Cryptographic Module | The private key of the scheme or of a CSP accredited under the scheme should be generated and retained in the cryptographic module or held in encrypted form in a secure device used for key transport.<br><br>Where key backup or restoration may require transfer of a private key to or from the cryptographic module this should be subject to the same controls as generation of an original key. |
| 6.2.7 Private Key Storage in Cryptographic Module | 6.2.6 Private Key Entry into Cryptographic Module | The private key of the scheme or of a CSP accredited under the scheme should be generated and retained in the cryptographic module.<br><br>Cryptographic modules used by the scheme, CAs or CMAs should meet the requirements of, or equivalent to FIPS 140-1 level 3.<br><br>Cryptographic modules used by RAs or RSPs accredited under the scheme should meet the requirements of, or equivalent to, FIPS 140-1 level 2. |
| 6.2.8 Method of Activating Private Key | 6.2.7 Method of Activating Private Key | Activation of the private key of the scheme or of a CSP accredited under the scheme should be subject to an approved access control method.<br><br>Initial activation of a private key generated for a subject should require the use of activation data provided to the subject via a separate channel to that used to provide the key.<br><br>Subjects should be required to use activation data when using the private key for signing. Consideration could be given to providing keys in a form that requires such activation. |
| 6.2.9 Method of Deactivating Private Key | 6.2.8 Method of Deactivating Private Key | Private keys should be automatically deactivated at the time |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | of shutdown or after a set period of inactivity.<br><br>Such processes should ensure that recoverable copies are not permitted to remain in any application, memory or disk space. |
| 6.2.10 Method of Destroying Private Key | 6.2.9 Method of Destroying Private Key | Where destruction of a private key used only for signing is permitted under applicable law, such keys should be destroyed including any backed up copies. The procedures should ensure that recoverable copies are not retained in any memory, module or disk space, including any backups.<br><br>NOTE: Some jurisdictions that have implemented the OECD Guidelines for Cryptography Policy require the use of separate encryption and signing keys to allow law enforcement access to encryption keys without compromising signing keys. This issue may need to be addressed in cross recognition agreements. |
| 6.2.11 Cryptographic Module Rating | 6.2.1 Standards for Cryptographic Modules<br><br>6.8 Cryptographic Module Engineering Controls | Cryptographic modules used by the scheme, CAs or CMAs should meet the requirements of, or equivalent to FIPS 140-1 level 3.<br><br>Cryptographic modules used by RAs or RSPs accredited under the scheme should meet the requirements of, or equivalent to, FIPS 140-1 level 2.<br><br>Cryptographic modules used by subjects under the scheme should meet the requirements of, or equivalent to, FIPS 140-1 level 1.<br><br>Proposed standard ISO/IEC 19790 based on FIPS 140-2 is being developed to address this requirement.<br><br>NOTE: ISO/IEC 15408 based Protection Profiles for cryptographic devices certified EAL4+ are defined in: CWA 14169 (subjects' devices), CWA 14167-2 and –4 for CAs, TSAs, etc. signing, CWA 14167-3 for key generation outside the signing device.<br><br>CEN Workshop Agreements (CWAs) 14169, 14167-2, 14167-3, 14167-4 are ISO 15408 - Common Criteria - compliant Protection Profiles for signing devices developed by a CEN (Comité Européen de Normalisation- www.cenorm.be) Workshop within the European Electronic Signature Specification Initiative. These documents can be accessed at URL http://www.cenorm.be/cenorm/businessdomains/businessdomains/isss/cwa/electronic+signatures.asp.<br><br>TSA: Time Stamping Authority: authority which issues time-stamp tokens (RFC 3628) |
| 6.3 Other Aspects of Key Pair Management | 6.3 Other Aspects of Key Pair Management | |
| 6.3.1 Public Key Archival | 6.3.1 Public Key Archival | Public keys should be archived in accordance with the records archival policy. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 6.3.2 Certificate Operational Periods and Key Pair Usage Periods | 6.3.2 Usage Periods for the Public and Private Keys | The maximum usage period for a private key should be determined by the risk of compromise of a key of that strength and may need to be varied in the light of technological advances.<br><br>At this stage a Scheme or CSP 2048 bit signing key should have a maximum usage period of the certificate life cycle or ten years, whichever is the lower. A subscriber 1024 bit key should have a maximum usage period of the certificate life cycle or of three years, whichever is the lower.<br><br>Current vulnerability assessments[3] indicate that RSA and DSA 1024 bit or elliptic curve 160 bit key lengths should not be used beyond 2010 and RSA and DSA 2048 bit or elliptic curve 224 bit key lengths should not be used beyond 2030.<br><br>Certificate operational periods should not exceed the appropriate key pair usage period or the identity data re-validation period.<br><br>Confirmation of identity information relating to a certificate such as current operation of an organisation, current business name registration or current domain name ownership may be undertaken within a certificate operational period without the need to issue new certificates<br><br>NOTE: Schemes may implement longer key usage periods on the basis of an independent risk assessment. That assessment will need to be considered as part of the cross recognition process. |
| 6.4 Activation Data | 6.4 Activation Data | The scheme should document in its CP or other relevant documentation requirements for activation data under the scheme.<br><br>Where subjects are required to use activation data this should be recorded or referenced in the subscriber agreement. |
| 6.4.1 Activation Data Generation and Installation | 6.4.1 Activation Data Generation and Installation | Activation data requirements should be commensurate with the value of assets protected by the private key and any other access controls to that key.<br><br>Activation data generation may be user selected. |
| 6.4.2 Activation Data Protection | 6.4.2 Activation Data Protection | Activation data should be protected commensurate with the value of assets protected by the private key.<br><br>Suspension after a predetermined number of attempts should be supported. |
| 6.4.3 Other Aspects of Activation Data | 6.4.3 Other Aspects of Activation Data | The life cycle of activation data should be commensurate with the value of assets protected by the private key.<br><br>As an example, PINs and passwords may be required to be |

[3] RSA assessment is at http://www.rsasecurity.com/rsalabs/node.asp?id=2004
NIST assessment is at http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | changed every 30 days with limitations on format and use. |
| 6.5 Computer Security Controls | 6.5 Computer Security Controls | The scheme should set out in its CP or other relevant documentation the required computer security controls for the scheme and CSPs accredited under the scheme, including methods to assess the implementation of those controls.<br>ISO/IEC 17799 "Information technology – Code of practice for information security management" and ISO/IEC TR13335 "Information technology -- Guidelines for the management of IT Security" can provide guidance on the types of controls that should be implemented.<br>ISO/IEC 15408 "Information technology -- Security techniques -- Evaluation criteria for IT security" can be used to evaluate technology used in a PKI operation. |
| 6.5.1 Specific Computer Security Technical Requirements | 6.5.1 Specific Computer Security Technical Requirements | ISO/IEC 17799 "Information technology – Code of practice for information security management" and ISO/IEC TR13335 "Information technology -- Guidelines for the management of IT Security" can provide guidance on the types of controls that should be implemented.<br>ISO/IEC 15408 "Information technology -- Security techniques -- Evaluation criteria for IT security" can be used to evaluate technology used in a PKI operation. |
| 6.5.2 Computer Security Rating | 6.5.2 Computer Security Rating | The assessment or evaluation should use recognised standards and be to a level set out by the scheme.<br>ISO/IEC 15408 "Information technology -- Security techniques -- Evaluation criteria for IT security" can be used to evaluate technology used in a PKI operation.<br>As a minimum, components, other than subject or relying party components, should be rated EAL4 or equivalent. |
| 6.6 Life Cycle Technical Controls | 6.6 Life Cycle Technical Controls | |
| 6.6.1 System Development Controls | 6.6.1 System Development Controls | The scheme should document in its CP or other relevant documentation any system development controls.<br>Software and hardware should be subject to quality assurance controls in its development within the scheme or commercially.<br>Software, hardware and configurations should be verified in a test environment before going into operation. |
| 6.6.2 Security Management Controls | 6.6.2 Security Management Controls | Controls should be in place to prevent or detect unauthorised modification of software or changes in system configuration.<br>Validation of system integrity should be undertaken once per week. |
| 6.6.3 Life Cycle Security Controls | 6.6.3 Life Cycle Security Ratings | Security controls should be reviewed as part of the audit or assessment of compliance with the scheme. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 6.7 Network Security Controls | 6.7 Network Security Controls | Cryptographic modules containing private keys used for signing CSP and cross certificates should not be connected to any open network.<br><br>Where repositories of certificates, public keys, cross certificates or status information are connected to open networks they should be subject to network security controls including firewalls. Configured to only allow operations necessary to the functioning of the scheme.<br><br>ISO/IEC 17799 "Information technology – Code of practice for information security management" and ISO/IEC TR13335 "Information technology -- Guidelines for the management of IT Security" can provide guidance on the types of controls that should be implemented. |
| 6.8 Time-Stamping | No Provision | The scheme should record whether time and date stamping services are supported. ISO/IEC 18014-1:2002 "Information technology -- security techniques -- Time-stamping services -- Part 1: Framework" can provide guidance on time-stamping. A trusted time source should be utilised.<br><br>Repository information such as directories, CRL's and status information, including archived copies should indicate the time and date of generation or issue.<br><br>"RFC 3126 "Electronic Signature Formats for long term electronic signatures" can also provide guidance. |
| 7. CERTIFICATE, CRL AND OCSP PROFILES | 7. CERTIFICATE AND CRL PROFILES | The scheme should document in its CP or other documentation the certificate and CRL profiles applicable for the scheme. |
| 7.1 Certificate Profile | 7.1 Certificate Profile | The scheme should support the X509 v3 certificate profile as implemented in RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificate Profile.<br><br>Where non standard extensions are used it should be recognised that such extensions can prevent applications in other schemes processing the certificate.<br><br>Where a scheme or group of schemes is operating on a closed basis other profiles may be considered. |
| 7.1.1 Version Number(s) | 7.1.1 Version Number(s) | X.509 v3 should be supported and used. |
| 7.1.2 Certificate Extensions | 7.1.2 Certificate Extensions | The scheme should support and use X.509 v3 certificate extensions. |
| 7.1.3 Algorithm Object Identifiers | 7.1.3 Algorithm Object Identifiers | Algorithm OIDs should conform with RFC 3279 and RFC 3280 |
| 7.1.4 Name Forms | 7.1.4 Name Forms | Name forms should be in theX.500 distinguished name format as implemented in RFC 3039. |
| 7.1.5 Name Constraints | 7.1.5 Name Constraints | Name constraints should be supported as per RFC 3280. |
| 7.1.6 Certificate Policy Object Identifier | 7.1.6 Certificate Policy Object Identifier | Certificate policy object identifiers should be used as per |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | RFC 3039<br><br>Qualified certificate statements as per RFC 3039 should also be supported. |
| 7.1.7 Usage of Policy Constraints Extension | 7.1.7 Usage of Policy Constraints Extension | Policy constraints should be supported as per RFC 3280. |
| 7.1.8 Policy Qualifiers Syntax and Semantics | 7.1.8 Policy Qualifiers Syntax and Semantics | The use of the policy qualifiers defined in RFC 3280 should be supported. |
| 7.1.9 Processing Semantics for the Critical Certificate Policy Extension | 7.1.9 Processing Semantics for the Critical Certificate Policy Extension | The scheme should be able to accept certificates containing any of the standard extension defined in RFC 3280 whether marked critical or not.<br><br>Schemes should avoid marking non-standard extensions as critical in certificates intended for use outside the scheme. |
| 7.2 CRL Profile | 7.2 CRL Profile | The scheme should document in its CP or other relevant documentation the CRL profiles it supports. |
| 7.2.1 Version Number(s) | 7.2.1 Version Number(s) | As a minimum X.509 v2 CRLs should be used. X.509 v3 should be supported. |
| 7.2.2 CRL and CRL Entry Extensions | 7.2.2 CRL and CRL Entry Extensions | The scheme should support the CRL extensions defined in RFC 3280. |
| 7.3 OCSP Profile | No Provision | The scheme should document in its CP or other relevant documentation whether OCSP is supported.<br><br>IETF RFC 2560 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP” provides guidance on the data exchange when using OCSP. |
| 7.3.1 Version Number(s) | No Provision | The scheme should document in its CP or other relevant documentation the OCSP Version Numbers that may be supported. |
| 7.3.2 OCSP Extensions | No Provision | The scheme should support the CRL extensions defined in RFC 2560. |
| 8. COMPLIANCE AUDITS AND OTHER ASSESSMENTS | 2.7 Compliance Audit | The scheme should be subject to independent compliance audit or assessment in respect of its operations. The frequency of such compliance audits or assessments and the process for publication of the outcomes should be recorded in the scheme’s CP or other relevant documentation.<br><br>The compliance audit or assessment process required to obtain and retain accreditation under the scheme should be recorded in the scheme’s CP or other documentation. |
| 8.1 Frequency and Circumstances of Assessment | 2.7.1 Frequency of Entity Compliance Audit | CSPs accredited under the scheme should be compliance audited or assessed for compliance with the scheme once per year.<br><br>CSPs may also undergo independent compliance audit or assessment for compliance with their CP and CPS.<br><br>The results of the compliance audits or assessments should be published. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 8.2 Identity/Qualifications of Assessor | 2.7.2 Identity/Qualifications of Auditor | A compliance audit or assessment team should include persons who possess significant experience with information technologies, security, PKI and cryptographic technologies<br><br>The scheme may require that persons undertaking audits or assessments of compliance with the scheme be approved by the scheme. |
| 8.3 Auditor's Relationship to Audited Entity | 2.7.3 Auditor's Relationship to Audited Party | Compliance auditors or assessors should be independent of the organisation being audited or assessed. |
| 8.4 Topics Covered by Assessment | 2.7.4 Topics Covered by Audit | The scheme should specify the elements of an audit or assessment of compliance with the scheme.<br><br>The framework set out in RFC 3647 may be used to develop a minimum set of elements. |
| 8.5 Actions Taken as a Result of Deficiency | 2.7.5 Actions Taken as a Result of Deficiency | The scheme should specify actions to be taken as a result of a deficiency.<br><br>The scheme should include the right to revoke or suspend CSP accreditation where there are significant deficiencies in an audit or assessment of compliance with the scheme. |
| 8.6 Communication of Results | 2.7.6 Communication of Results | The results of the compliance audit or assessment of a scheme should be published at the same location as the CP or other relevant documentation on the scheme.<br><br>The results of audits or assessment of compliance with the scheme of CSPs accredited under the scheme should be published as part of the status information of those bodies published by the scheme.<br><br>Where a scheme recognises certificates issued by other schemes the results of compliance audits or assessments of those schemes and CSPs accredited under them should be published by the scheme as part of the status information of those schemes. |
| 9. OTHER BUSINESS AND LEGAL MATTERS | 2. GENERAL PROVISIONS | |
| 9.1 Fees | 2.5 Fees | The scheme should identify where fees are payable for participation in the scheme.<br><br>A CSP should record fees payable in it CP and other relevant documentation. In particular fees should be recorded or referenced in agreements with subscribers and relying parties. |
| 9.1.1 Certificate Issuance or Renewal Fees | 2.5.1 Certificate Issuance or Renewal Fees | Where a scheme requires issue of a certificate to CSPs accredited under the scheme, the scheme should identify any fees that are payable.<br><br>A CSP should record fees payable in it CP and other relevant documentation. In particular fees should be recorded or referenced in agreements with subscribers and relying parties. |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 9.1.2 Certificate Access Fees | 2.5.2 Certificate Access Fees | Where a scheme issues a certificate to CSPs accredited under the scheme, any fees for access to that certificate should be recorded.<br><br>A CSP should record fees payable in it CP and other relevant documentation. In particular fees should be recorded or referenced in agreements with subscribers and relying parties. |
| 9.1.3 Revocation or Status Information Access Fees | 2.5.3 Revocation or Status Information Access Fees | Where a scheme issues a certificate to CSP accredited under the scheme, any fees for access to status information on that certificate should be recorded.<br><br>A CSP should record fees payable in it CP and other relevant documentation. In particular fees should be recorded or referenced in agreements with subscribers and relying parties.<br><br>It should be noted that charging for status or revocation information may discourage relying parties from validating certificates and should be avoided where possible |
| 9.1.4 Fees for Other Services | 2.5.4 Fees for Other Services Such as Policy Information | A scheme should record any fees payable for access to policy information on the scheme.<br><br>A CSP should record fees payable in it CP and other relevant documentation. In particular fees should be recorded or referenced in agreements with subscribers and relying parties. |
| 9.1.5 Refund Policy | 2.5.5 Refund Policy | A CSP should record its refund policy in it CP and other relevant documentation. In particular the policy should be recorded or referenced in agreements with subscribers and relying parties. |
| 9.2 Financial Responsibility | 2.3 Financial Responsibility | The scheme should record the requirements for financial responsibility for CSPs accredited under the scheme.<br><br>In particular the scheme should ensure that a CSP has the resources to operate in accordance with its CP and CPS including any warranty or liability provisions.<br><br>CSPs should record their financial responsibilities in their CP or other relevant documentation in accordance with RFC 3647.<br><br>Where a CA outsources part of its operations, the financial responsibility requirements of those operations should be recorded. |
| 9.2.1 Insurance Coverage | 2.3 Financial Responsibility | The scheme should record the requirements, if any, for insurance coverage for CSPs accredited under the scheme. |
| 9.2.2 Other Assets | 2.3 Financial Responsibility | The scheme should record any minimum asset requirements for CSPs accredited under the scheme.<br><br>Details of actual assets should not be published by the |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | scheme. |
| 9.2.3 Insurance or Warranty Coverage for End-Entities | 2.3 Financial Responsibility | The scheme should record the requirements, if any, for insurance coverage or warranty protection for subscribers and relying party.<br><br>Where insurance coverage or warranty protection is available to subscribers this should be recorded or referenced in the subscriber agreement, including terms and conditions for the subscriber coverage.<br><br>Where insurance coverage or warranty protection is available to relying parties this should be recorded or referenced in PKI disclosure statement or similar documentation, including terms and conditions for the relying party coverage. |
| 9.3 Confidentiality of Business Information | 2.8 Confidentiality | The scheme should specify the categories of information that is to be kept confidential.<br><br>The scheme should ensure that accredited CSPs comply with applicable data protection, information confidentiality and intellectual property laws. |
| 9.3.1 Scope of Confidential Information | 2.8.1 Types of Information to be Kept Confidential<br><br>2.8.3 Disclosure of Certificate Revocation/Suspension Information | The scheme should ensure that information it holds relating to the commercial operations or intellectual property of accredited CSPs is kept confidential.<br><br>The scheme should ensure that CSPs accredited under the scheme ensure that the following information is kept confidential:<br><br>• "Commercial in confidence" material of CSPs and business subscribers and relying parties, including contractual terms, business plans and intellectual property;<br><br>• Information that would allow unauthorised parties to establish the existence or nature of relationships between business subscribers and relying parties; and<br><br>• Information that would allow unauthorised parties to construct a profile of subscribers, subjects or relying parties' activities.<br><br>The scheme should ensure that information it holds that may prejudice the security of operation of the scheme is kept confidential.<br><br>The scheme should permit the publication of information on whether a certificate has been suspended or revoked without revealing the reason for suspension or revocation.<br><br>Publication may be limited to legitimate subscribers, subjects and relying parties to the scheme or any other recognised scheme. |
| 9.3.2 Information Not Within the Scope of | 2.8.2 Types of Information Not | The scheme should permit the publication of certificates and certificate status information and of information on whether |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| Confidential Information | Considered Confidential<br><br>2.8.3 Disclosure of Certificate Revocation/Suspension Information | a certificate has been suspended or revoked without revealing the reason for suspension or revocation.<br><br>Publication may be limited to legitimate subscribers, subjects and relying parties to the CA domain, the scheme or any other recognised scheme. |
| 9.3.3 Responsibility to Protect Confidential Information | 2.8 Confidentiality<br><br>2.8.3 Disclosure of Certificate Revocation/Suspension Information<br><br>2.8.4 Release to Law Enforcement Officials<br><br>2.8.5 Release as Part of Civil Discovery<br><br>2.8.6 Disclosure Upon Owner's Request<br><br>2.8.7 Other Information Release Circumstances | The scheme should specify the categories of information that are to be kept confidential and the circumstances in which such information can be released.<br><br>The scheme should ensure that accredited CSPs comply with its confidentiality requirements and with applicable data protection, information confidentiality and intellectual property laws. |
| 9.4 Privacy of Personal Information | 2.8 Confidentiality | The scheme and CSPs accredited under the scheme should comply with relevant personal data protection legislation in the jurisdiction within which the scheme is established.<br><br>Consideration should also be given to personal data protection legislation of jurisdictions where other schemes with which a cross-recognition agreement exists are located and to the personal data protection policies of those schemes. Particular attention should be given to provisions relating to the cross-border transfer of personal information.<br><br>The scheme should undertake a privacy impact assessment of the scheme and should require CSPs to undertake a privacy impact assessment of their operations as part of the CSP accreditation process. |
| 9.4.1 Privacy Plan | No provision | The scheme should develop a privacy plan for the scheme and should require CSPs to prepare a privacy plan as part of the documentation assessed in the CSP accreditation process.<br><br>The plan should address the type of personal data that can be collected, how it will be used, how it will be protected, how it can be reviewed/corrected, circumstances in which it will be disclosed and sanctions for failure to comply with the plan.<br><br>NOTE: The content of the plan, including sanctions, may impact the ability to undertake cross-border transfer of personal data between schemes. |
| 9.4.2 Information Treated as Private | 2.8.1 Types of Information to be Kept Confidential | The scheme should ensure that CSPs accredited under the scheme ensure that the following information is kept |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | 2.8.3 Disclosure of Certificate Revocation/Suspension Information | confidential:<br>• Personal information provided by subscribers, subjects and relying parties other than that authorised to be contained in certificates and repositories;<br>• Information that would allow unauthorised parties to establish the existence or nature of relationships between subscribers, subjects and relying parties; and<br>• Information that would allow unauthorised parties to construct a profile of subscribers, subjects or relying parties' activities.<br>The scheme should permit the publication of information on whether a certificate has been suspended or revoked without revealing the reason for suspension or revocation.<br>Publication may be limited to legitimate subscribers, subjects and relying parties to the CA domain, the scheme or any other recognised scheme. |
| 9.4.3 Information Not Deemed Private | 2.8.2 Types of Information Not Considered Confidential<br>2.8.3 Disclosure of Certificate Revocation/Suspension Information | The scheme should ensure that only personal information, the release of which has the explicit consent of the individual to whom that information relates, is disclosed.<br>The scheme should permit the publication of certificates and certificate status information and the publication of information on whether a certificate has been suspended or revoked without revealing the reason for suspension or revocation.<br>Publication may be limited to legitimate subscribers and relying parties to the CA domain, the scheme or any other recognised scheme. |
| 9.4.4 Responsibility to Protect Private Information | 2.8 Confidentiality<br>2.8.1 Types of Information to be Kept Confidential<br>2.8.3 Disclosure of Certificate Revocation/Suspension Information | The scheme should specify the categories of personal information that are to be kept confidential and the circumstances in which such information can be released.<br>The scheme should ensure that accredited CSPs comply with its confidentiality requirements and with applicable data protection and information confidentiality laws. |
| 9.4.5 Notice and Consent to Use Private Information | No Provision | The scheme should ensure that subscriber agreements address the type of personal data that can be collected, how it will be used, how it will be protected, how it can be reviewed/corrected, circumstances in which it will be disclosed, avenues for redress and sanctions for failure to comply with the agreement by the party or parties collecting or using the data. Explicit consent for the release of the specified data should be incorporated in the agreement.<br>PKI disclosure statements or other relevant notifications to relying parties should specifically address the type of personal data that may be collected, how it will be used, how it will be protected, how it can be reviewed/corrected, |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | circumstances in which it will be disclosed, avenues for redress and sanctions for failure to comply with the plan. Where possible explicit consent for the release of the specified data should obtained. Where this is not possible, the relying party should be informed that access to the material sought will constitute implicit consent.<br><br>NOTE: The content of the agreements or notifications, including sanctions, may impact the ability to undertake cross-border transfer of personal data between schemes. |
| 9.4.6 Disclosure Pursuant to Judicial or Administrative Process | 2.8.4 Release to Law Enforcement Officials<br><br>2.8.5 Release as Part of Civil Discovery | The scheme should permit the release of personal information to law enforcement officials or as part of civil discovery where a request is made is in accordance with applicable law in the jurisdiction in which an accredited CSP is located.<br><br>Where a request for release of information comes from outside that jurisdiction it should be permitted where appropriate mutual assistance laws are complied with. |
| 9.4.7 Other Information Disclosure Circumstances | 2.8.6 Disclosure Upon Owner's Request<br><br>2.8.7 Other Information Release Circumstances | The scheme should permit subscribers, subjects and relying parties to request the release to other parties of information they have provided.<br><br>The scheme should require that the release of information in other circumstances is only in accordance with the scheme's CP or other relevant documentation and is in accordance with applicable law. |
| 9.5 Intellectual Property Rights | 2.9 Intellectual Property Rights | The scheme should ensure necessary access to registration information, names, keys, certificates and repository information, including archive copies is available to allow continuation of scheme in the event of withdrawal or failure of a CSP accredited under the scheme. This may involve intellectual property issues.<br><br>The scheme should permit CSPs accredited under the scheme to retain intellectual property in respect of their own technology and processes.<br><br>The scheme should ensure that CSPs accredited under the scheme hold the necessary intellectual property rights for material and processes they utilise in their operations under the scheme. |
| 9.6 Representations and Warranties | 2.2 Liability | The scheme should ensure that that the warranties and liability of CSPs accredited under the scheme and any limitations on the liability is recorded in the CP or other relevant documentation of the CSP.<br><br>The scheme should also record its own warranties and liability in respect of errors and omissions in the CSP accreditation process and any limitations or transfer of that liability. |
| 9.6.1 CA Representations and Warranties | 2.2.1 CA Liability | The CA should record any warranties and liability provisions, including limitations and exclusions in its CP. It |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | should also ensure that the provisions are included in any subscriber or relying party agreement or documentation and in any PKI disclosure statement.<br><br>Where a CA outsources RA or Repository functions, the liability of the CA and that of the organisations undertaking the outsourced activities should be recorded. The CA should record the liability provisions in respect of errors and omissions in ensuring that the organisations undertaking the outsourced activities are doing so in accordance with the CA's CP, CPS and other documentation.<br><br>In particular the CA should address liability in respect of errors and omissions in the production and distribution of certificates, directories and certificate revocation lists, including the availability of those directories and CRLs. |
| 9.6 2 RA Representations and Warranties | 2.2.2 RA Liability | The RA should record any warranties and liability provisions, including limitations and exclusions in its CP or other documentation. It should also ensure that the provisions are included in any subscriber or relying party agreement or documentation and in any PKI disclosure statement. The CA and the scheme should record in their CP and CPS their liability in respect of the operations of the RA.<br><br>In particular the CA and the RA should address liability in respect of errors and omissions in subscriber identification, processing of certificate or certification revocation requests and protection of personal information provided. |
| 9.6.3 Subscriber Representations and Warranties | 2.1.3 Subscriber Obligations | A subscriber or subject should be required to comply with subscriber obligations set out by the scheme or in the CP and CPS of the CA.<br><br>The subscriber should be required to sign an agreement to comply with their obligations, including those of subjects enrolled by the subscriber. The agreement should include any consequences of failure to comply with the agreement.<br><br>Where legislation places certain obligations on subscribers or subjects to ensure the legal effect of transactions utilising certificates issued by the CA the subscriber agreement should record those obligations.<br><br>Where a jurisdiction places obligations on subscribers to, or subjects of, schemes outside that jurisdiction those obligations should be made available to those subscribers or subjects.<br><br>The subscriber or subject obligations may include warranting the accuracy of information provided in certificate applications, agreeing to protect keys and certificates from misuse and agreeing not to use keys and certificates outside the scope of the scheme.<br><br>Where a subscriber enters an agreement on behalf of a number of subjects, its responsibilities in respect of the |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | actions of those subjects should be recorded. |
| 9.6.4 Relying Party Representations and Warranties | 2.1.4 Relying Party Obligations | A relying party should be required to comply with relying party obligations set out by the scheme or in the CP and CPS of the CA.<br><br>The relying party should be notified of their obligations by way of a PKI disclosure statement or similar document published and made accessible to the relying party. The statement or document should include any consequences of failure to comply with the agreement.<br><br>Where legislation places certain obligations on a relying party to ensure the legal effect of transactions utilising certificates relied on by the relying party, the documentation should record those obligations.<br><br>The relying party obligations may include checking the status of certificates and agreeing not to use certificates outside the scope of the scheme. |
| 9.6.5 Representations and Warranties of Other Participants | Repository Liability | The Repository and any other participants not specifically mentioned above should record any warranties and liability provisions, including limitations and exclusions in its CP or other documentation. It should also ensure that the provisions are included in any subscriber or relying party agreement or documentation and in any PKI disclosure statement. The CA and the scheme should record in their CP and CPS their liability in respect of the operations of the Repository and any other participants not specifically mentioned above.<br><br>In particular the CA and the Repository should address liability in respect of errors and omissions in processing and maintaining directories and CRLs and in the availability of those repositories. |
| 9.7 Disclaimer of Warranties | 2.2 Liability<br><br>2.3.2 Fiduciary Relationships | The scheme and CSPs should record any disclaimer of warranties in their CP, CPS and other relevant documentation. It should also ensure that the provisions are included in any subscriber or relying party agreement or documentation and in any PKI disclosure statement.<br><br>The scheme may specify warranties that cannot be disclaimed. |
| 9.8 Limitations of Liability | 2.2 Liability | The scheme and CSPs should record any limitations of liability in their CP, CPS and other relevant documentation. It should also ensure that the provisions are included in any subscriber or relying party agreement or documentation and in any PKI disclosure statement.<br><br>The scheme may specify maximum levels of liabilities applicable in specific circumstances. |
| 9.9 Indemnities | 2.1.3 Subscriber Obligations<br><br>2.1.4 Relying Party | The scheme and CSPs should record any indemnities in their CP, CPS and other relevant documentation. It should also ensure that the provisions are included in any subscriber or relying party agreement or documentation and in any PKI |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | Obligations<br><br>2.2 Liability<br><br>2.3.1 Indemnification by Relying Parties | disclosure statement.<br><br>The scheme may specify any limitations on seeking or obtaining indemnities. |
| 9.10 Term and Termination | No Provision | The scheme should record the term of validity of documentation of the scheme and of CSPs accredited under the scheme and circumstances under which the documentation can be terminated. Where a CSP operates both within and outside the scheme, term and termination need only apply to elements of the documentation relating to the scheme.<br><br>The scheme may require certain term and termination provisions be included in any subscriber and relying party agreements. |
| 9.10.1 Term | No Provision | The term of validity of documentation of CSPs accredited under the scheme should be subject to continuing accreditation under the scheme. Where CSP operates both within and outside the scheme, term and termination need only apply to elements of the documentation relating to the scheme. |
| 9.10.2 Termination | No Provision | Where a CSP accreditation under the scheme is terminated, its documentation should be terminated. Where a CSP operates both within and outside the scheme, term and termination need only apply to elements of the documentation relating to the scheme.<br><br>The scheme should allow subscriber and relying party agreements to be terminated where parties to the agreement fail to meet their obligations under the scheme. |
| 9.10.3 Effect of Termination and Survival | No Provision | The scheme should record severability, survival, and merger requirements applying to the rules of the scheme and any requirements the scheme places on CSPs accredited under the scheme.<br><br>A CSP should record severability, survival, and merger provisions in its CP or other relevant documentation, including subscriber and relying party agreements.<br><br>Differences in governing law could result in different provisions within a scheme. |
| 9.11 Individual Notices and Communications with Participants | 2.4.2 Severability, Survival, Merger, Notice | The scheme should record notice and communication requirements applying to the rules of the scheme and any requirements the scheme places on CSPs accredited under the scheme.<br><br>A CSP should record notice and communication provisions in its CP or other relevant documentation, including subscriber and relying party agreements. |
| 9.12 Amendments | 8.1 Specification Change Procedures | |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| 9.12.1 Procedure for Amendment | 8.1 Specification Change Procedures | The scheme should ensure that stakeholders in a scheme, including other schemes that recognise the scheme are consulted prior to any changes to the scheme. This provision does not necessarily apply to any changes to the policy and practices of a CSP accredited under the scheme where those changes remain consistent with the documented operations of the scheme itself.<br><br>The scheme should review any changes in the documented policy and practices of CSPs accredited under the scheme before they are implemented. The appropriate documentation may require revision. |
| 9.12.2 Notification Mechanism and Period | 8.1 Specification Change Procedures | The scheme may require any changes to the policies and practices of a CSP accredited under the scheme to be notified to subscribers, relying parties and other parties such as other schemes that recognise the scheme or cross certified CAs where they may be impacted by the changes.<br><br>Any changes to the basic terms and conditions (policy identifier, limitations of use, subscriber obligations, how to validate a certificate, limitations of liability, dispute resolution procedure, period which registration and audit logs are retained, applicable legal system and conformance to scheme) should notified to subscribers and relying parties.<br><br>The scheme, and CSPs accredited under the scheme, should advise subscribers and potential relying parties of the form of notification and the implications of that form of notification. |
| 9.12.3 Circumstances Under Which OID Must be Changed | 8.1 Specification change procedures | The scheme should ensure that any changes that could impact the use or acceptability of certificates under the scheme are recorded and a new OID assigned where applicable.<br><br>Version controls should be used to ensure that the applicable policy and practices at the time of an archived transaction can be established. |
| 9.13 Dispute Resolution Provisions | 2.4.3 Dispute Resolution Procedures | The scheme should record dispute resolution processes, including cross-jurisdictional dispute resolution services, applying in respect of the scheme.<br><br>The scheme should ensure that CAs or RAs accredited under the scheme have a name claim dispute resolution procedure. A CSP accredited under the scheme should record dispute resolution processes in its CP and other relevant documentation. Different governing laws may result in differing dispute resolution processes.<br><br>Where possible, and permitted under governing law, the use of on-line dispute resolution processes should be considered. |
| 9.14 Governing Law | 2.4.1 Governing Law | The scheme should identify the governing law applying to the scheme.<br><br>A CSP accredited under the scheme should identify in its CP |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| | | and other documentation the governing laws applying to its operations as well as the governing law applying to the scheme. Significant governing law requirements should be recorded or referenced in subscriber and relying party agreements.<br><br>In federations the governing law for the scheme may be different to the governing law nominated by a CSP. |
| 9.15 Compliance with Applicable Law | 2.4.1 Governing Law | The scheme should ensure that relevant laws applicable to the operations of the scheme are identified in its CP or other relevant documentation.<br><br>A CSP accredited under the scheme should identify in its CP and other documentation the laws applying to its operations. Significant applicable law requirements should be recorded or referenced in subscriber and relying party agreements.<br><br>In federations the applicable law for the scheme may be different to the applicable law for a CSPs, subscribers, subjects or relying parties. |
| 9.16 Miscellaneous Provisions | 2.4 Interpretation and Enforcement | The scheme should record in its CP or other relevant documentation any miscellaneous provisions applying to the scheme.<br><br>A CSP accredited under the scheme should include in its CP and other documentation any miscellaneous provisions applying to its operations under the scheme. Where appropriate these provisions should be recorded or referenced in subscriber and relying party agreements. |
| 9.16.1 Entire Agreement | 2.4.2 Severability, Survival, Merger, Notice | The scheme should reference in any accreditation agreement for CSPs accredited under the scheme any other documentation that may be incorporated in the agreement.<br><br>A CSP should reference in its subscriber and relying party agreement any other documentation that may be incorporated in the agreement. |
| 9.16.2 Assignment | No Provision | The scheme and CSPs accredited under the scheme should record in its documentation any limitation on assignment of rights or delegation of obligations.<br><br>Where a subscriber agreement covers multiple subjects, any limitation on assignment of rights or delegation of obligations to those subjects should be recorded in the agreement. |
| 9.16.3 Severability | 2.4.2 Severability, Survival, Merger, Notice | The scheme should reference in any accreditation agreement for CSPs accredited under the scheme any severability provisions that may apply to the agreement.<br><br>A CSP should reference in subscriber and relying party agreements any severability provisions that may apply to the agreement. |
| 9.16.4 Enforcement (Attorney's Fees and | 2.4.3 Dispute Resolution Procedures | The scheme should record in its CP or other relevant |

| RFC3647 SECTION | RFC2527 SECTION | RFC 3647 MODEL PROVISION |
|---|---|---|
| Waiver of Rights) | | documentation any enforcement provisions applying to the scheme.<br><br>A CSP accredited under the scheme should record in its CP and other documentation any enforcement provisions applying to its operations under the scheme. These provisions should be recorded or referenced in subscriber and relying party agreements. |
| 9.16.5 Force Majeure | No provision | The scheme should record in its CP or other relevant documentation whether "Force Majeure" provisions can be included in agreements under the scheme. In some cases "Force Majeure" provisions may be limited by requirements for CSP accreditation under the scheme for business continuity plans to address events that may be considered "Force Majeure".<br><br>CSPs should ensure "Force Majeure" provisions are explicitly recorded in subscriber and relying party agreements. |
| 9.17 Other Provisions | No Provision | The scheme should record in its CP or other relevant documentation any other provisions applying to the scheme.<br><br>A CSP accredited under the scheme should include in its CP and other documentation any other provisions applying to its operations under the scheme. Where appropriate these provisions should be recorded or referenced in subscriber and relying party agreements. |
| 10. Bibliography<br>[Not an RFC 3647 provision] | | The CP, CPS and other relevant documentation should provide references to documents used in the development of the documentation. Particularly those documents referenced in the documentation or which set a rule of law or regulation. |
| 11. Acronyms & Abbreviations<br>[Not an RFC 3647 provision] | | The CP, CPS and other relevant documentation should provide a list of acronyms and abbreviations used in the documentation |
| 12. Glossary<br>[Not an RFC 3647 provision] | | The CP, CPS and other relevant documentation should provide a list of terms for which definition may be required. |