PKI Certificates and Key Management Standard

Version: 1.0

Author: Public Key Management and Digital identity Section

Document Classification: Public

Published Date: December 2019

Document History:

Date	Issue	Status	Author
30/10/2019	0.1	First draft	PKI Team
03/11/2019	0.2	References and appendix A	PKI Team
06/11/2019	0.3	First Review	PKI Team
19/11/2019	0.4	Appendix B and C	PKI Team
05/12/2019	0.5	External Review	QCERT Team
08/12/2019	0.6	Second External Review	QCERT Team
15/12/2019	0.9	Document formatting	PKI Team
15/12/2019	1.0	Document Approval	Head of CSP-PMA

Content

I. Terms and Definitions

Auditor: person who assesses conformity to requirements as specified in given requirements documents.

Certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it. An electronic document that uses a electronic signature to bind a public key and an identity.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Revocation List (CRL)[1]: A regularly updated time-stamped list of revoked Certificates that is created and electronically signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Cross certificate: certificate that is used to establish a trust relationship between two certification authorities.

CSPRNG: A random number generator intended for use in cryptographic system

Electronic signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Pair: The Private Key and its associated Public Key

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system. Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create electronic Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Electronic Signatures

[1] Within the scope of the present standard the set of certificates is related to end user certificates.

created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure (PKI): A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate. Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

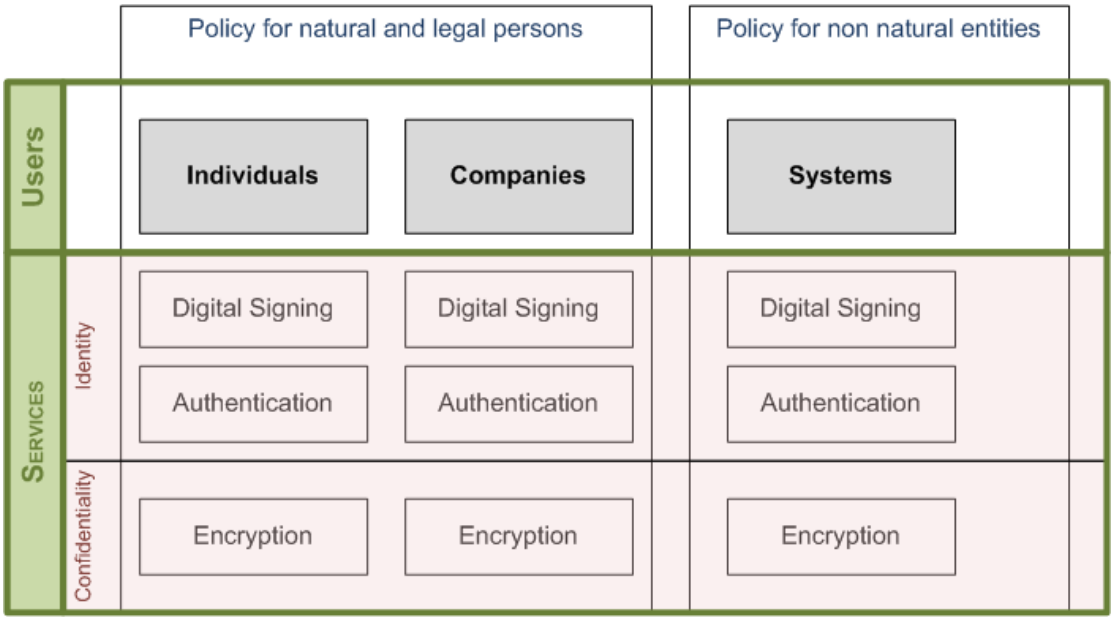
Trusted System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

II. Scope

This Standard defines the requirements for Certificate Service Providers [CSPs] issuing public key certificates. This standard is defined in terms of requirements for the issuance, maintenance and life-cycle management of certificates.

Hence this Standard is applicable to:

- Requirements of certification in support of cryptographic mechanisms, including electronic signatures and seals.
- Requirements of certification authorities issuing TLS/SSL certificates.
- Requirements of the use of cryptography for authentication and encryption.



The diagram described above illustrates the domains covered by a Certificate service provider. The solution and infrastructure supporting the PKI operations for CA certificates and digital signature certificates is described here as Trusted System.

III. Management

A CSP operating in Qatar MUST have a comprehensive security management program in order to manage properly the security of the PKI operated as a Trusted System.
CSP policies must outline the controls defined within the CSP organization, in-line with the Policy Management Authority of Qatar, the e-commerce law and related Qatar technical standards.
Security officers, registration officers, system administrators, operators and system auditors have been clearly defined and identified with separate roles, credentials and duties. Each function cannot be held by the same person. Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the CSP's assets.

A CSP MUST provide a fully transparent description of its services and the following items MUST be implemented to provide key and certificate management services:

- public key certificates
- CA repository
- Certificate revocation process
- Key backup and recovery
- Non-repudiation of digital signatures
- Updates of key pairs and certificates
- Key histories management
- cross-certification
- client software required to process operations

Related policies and procedures MUST cover the requirements for at least each of these components or more.

IV. Certificate Management Security Requirements

This section includes the provision of services for registration, certificate generation, dissemination, revocation management and revocation status. The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives where considered necessary to provide the necessary confidence that those objective will be met.

1. General Requirement

The present document is structured broadly in line with IETF RFC 3647 to assist CSPs in applying these requirements to their own CP and CPS documentation. CSPs shall document in detail, within their Certification Practice Statement, how they will meet the operational requirements for issuing and managing the certificates covered by this standard.
Operational requirements in the CPS must provide details on how certificate will be disseminated as well. Whether it is online or onsite, information on location for registration, issuance and revocation operations is required to ensure proper delivery to service end users.

1.1. Certification Practice Statement (CPS)

CSP shall specify the set of policies and practices appropriate for the trust services it is providing. The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.
CSP shall have a statement of the practices and procedures used to address all the requirements identified for the applicable CSP's policy.
In addition, the following particular requirements apply:

- CPS should be structured in accordance with IETF RFC 3647.
- CPS shall include the signature algorithms and parameters employed.
- CSP shall publicly disclose its CPS through an online means that is available on a 24x7 basis.
- CSP's certification practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices.
- The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to assess conformance to the service policy.
- CSP shall have a management body with overall responsibility for the TSP with final authority for approving the CSP's practice statement.
- CSP's management shall implement the practices.
- CSP shall define a review process for the practices including responsibilities for maintaining the CSP's practice statement.
- CSP shall notify notice of changes it intends to make in its practice statement.
- CSP shall state in its practices the provisions made for termination of service.

1.2. Certificate Policy (CP)

A CP is a higher-level document than a CPS; it can apply to a community to which several CAs belong that abide by the common set of rules specified in that CP. A CPS defines how one specific CSP meets the technical, organizational and procedural requirements identified in a CP. CP is defined as "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.

In particular, when the CSP issues a CP:

- The CSP should make available the CPs supported by the TSP to its user community.
- A unique object identifier shall be obtained for the CP.
- The CP shall specify the Recommendation ITU-T X.509 certificate profile requirements.
- A risk assessment should be carried out to evaluate business requirements and determine the security requirements to be included in the CP for the stated community and applicability.
- CP should be approved and modified in accordance with a defined review process, including responsibilities for maintaining the CP.
- A defined review process should exist to ensure that the CP is supported by the CSP's CPS.

2. Certificate Life-Cycle operational requirements

2.1. Certificate Registration, Application & Acceptance:

Subscribers may obtain certificates through any licensed CSP that has been approved to issue these certificates. A signed application form and a suitable subscriber agreement (incorporating this CP's obligations) must support the application process.

After initial registration and certification of their signing and authentication public keys, subscribers shall be issued with their keys and related certificates on a hardware device or using secure software key container.

After review of their certificate details, a subscriber's use of their keys/ certificates shall constitute an acceptance of the keys/certificates.

2.1.1. Identification and authentication

The CSP shall verify the identity of the subscriber and subject, and shall check that certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

- ***Initial identity validation***

The CSP shall verify the identity of the subscriber and subject. When registering, a subject is identified as a person with specific attributes. The specific attributes can indicate, for example, an association within an organization and possibly, a role within that organization. Identity validation is part of at least one of processes: certificate application, certificate issuance, subject device provisioning.
In particular:

- CSP shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the RA shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.
- If the subject is a natural person (i.e. physical person as opposed to legal person), evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

2.1.2. Certificate Application

A Registration Officer verifies by appropriate means, in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a certificate is issued.
If the certificate application contains any subject sensitive information, the certificate request MUST be protected before being forwarded from the Registration Service to the Certificate Generation Service thus ensuring message confidentiality. Trusted system MUST ensure this functionality is provided if required.
This service MUST implement a suitable mechanism to obtain proof of possession to ensure the entity requesting Certification is the actual holder of the private key related to the public key requiring Certification.
An example of this would be to include a signature block with each certificate application, which is created by the private key associated with the public key requiring Certification. Trusted system MUST provide a mechanism to allow approval of certificate applications, by a Registration Officer, before leaving the Registration Service.
Application for certificates shall be from a trusted registration service. In particular, When external registration service providers are used registration data shall be exchanged securely and only with recognized registration service providers, whose identity is authenticated.

2.1.3. Subject Data Management

The Registration Service by its nature MUST manage end entity subject data. The data may be affected by many different data protection requirements such as Qatar Data protection laws.

Trusted Systems SHALL implement mechanisms and security controls to protect the privacy and confidentiality of Subject information. All events related to the registration process MUST be logged for auditing purposes

2.2. Certificate Issuance Service

CSPs MUST ensure smooth operation in certificate delivery and generation. CSPs MUST have dedicated security controls from the initiation processes until the dissemination of certificates.

2.2.1. Certificate Issuance

After receiving a certificate application from the Registration Service, trusted system, generate a certificate using the public key supplied. This ensures the CSP has 'locked' the binding of the Subject's public key to its identity.

Following Certificate Generation, the certificate may be made available via the Dissemination Service, via the supplementary Subject Device Provision Service or to the Subject directly. Infrastructure and Control Certificates may be provided directly to the trustworthy component requiring its use.
The certificate generation service MUST ensure the integrity, data origin authenticity, and where necessary, the privacy and confidentiality of the certificate request message.
The certificate request MUST be processed securely and checked for conformance with the applicable Certificate Policy.
Before certificate generation, the trusted system MUST ensure Proof of Possession is validated. This service SHALL ONLY generate certificates that are consistent with the allowed profiles as determined by the Security Officer. All certificates issued by a trusted system MUST have the following properties:

- Indication of the subject's name or pseudonym. Where a pseudonym is used this MUST be clearly indicated.
- The public key in the certificate is related to the subject's private key.
- The advanced electronic signature of the CSP, created using the CSP Signing Keys.
- A unique distinguished name and serial number assigned by the trusted system. This MUST be unique with respect to the issuing CSP.
- The certificate SHALL specify a valid from time that does not precede the current time and a valid until time that does not precede the valid from time.
- The signature algorithms/keys used by the trusted system to sign the certificate MUST be conformant to the algorithm specifications standard.
- Reference to the Certificate Policy under which the certificate is issued.

2.2.2. Certificate Issuance Requirements

These clauses shall apply:

- The CA shall issue certificates securely to maintain their authenticity.
- The CA shall take measures against forgery of certificates.
- In cases where the CA generates the subjects' key pair, the CA shall guarantee confidentiality during the process of generating such data[2].
- The procedure of issuing the certificate shall be securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject-generated public key.

[2] Conditional clause

- The CSP should not issue certificates whose lifetime exceeds that of the CA's signing certificate.
- If the CSP does issue certificates whose lifetime exceeds the lifetime of the CA's signing certificate, the TSP shall ensure that the certificate status can still be verified by relying parties after expiry of the CA certificate[3].
- If the CA generates the subject's key pair, the procedure of issuing the certificate shall be securely linked to the generation of the key pair by the CA[4].
- If the CA generates the subject's key pair, the private key shall be securely handed to the registered subject; or to the CSP managing the subject's private key[5].
- If the CA generates the subject's key pair, the secure cryptographic device containing the subject's private key shall be securely delivered to the registered subject or, in the case of the CSP managing the key on behalf of the subject, the CSP shall ensure that the subject has sole control (or if the subject is a legal person "control") over its signing key[6].

2.3. Certificate Renewal

Renewal mechanism must be simple and clearly identified by the CSP. During the period prior to the expiration of the certificate, such period being defined by applicable policy, the certificate may be renewed. Requests for certificates issued to a subject who has previously been registered with the same CSP shall be complete, accurate and authorized. For example, the subscriber can, if the CSP offers this service, request a certificate renewal where relevant attributes presented in the certificate have not changed or when the certificate lifetime is nearing expiry. Existing evidences can be re-used to validate the identity depending on applicable legislation and whether the evidence remains valid given the time elapsed.

In Particular:

- The CSP shall check the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject are still valid.
- If any of the CSP's terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with requirements.
- The CA shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised nor that the certificate has been revoked due to any other security breach.

Trusted system MUST ensure Signing Keys are updated prior to their expiry. The related (renewed) public keys MUST provide at least the same level of trust as when they were initially distributed.

[3] Conditional clause
[4] Conditional clause
[5] Conditional clause
[6] Conditional clause

2.4. Certificate Rekey

Renewal mechanism must be simple and clearly identified by the CSP. Requests for certificates issued to a subject who has previously been registered with the same CSP shall be complete, accurate and authorized. This includes re-key following revocation or prior to expiration, or update due to change to the subject's attributes.

- The CSP shall check the existence and validity of the certificate to be rekeyed and that the information used to verify the identity and attributes of the subject are still valid.
- If any of the CSP's terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with requirements on the present document.

2.5. Cross Certification

This mechanism allows the establishing of a one-way or a mutual trust relationship between two (or more) CSPs. The responder trusted system provides a cross certificate to the requester trusted system who provides its public key for certification. The subjects of the responder CSP can now trust the requester CSP.

Where a trusted system uses cross-certification for establishing one-way or mutual trust with other trusted system, the process MUST ensure that:

- Authentication and integrity of messages are maintained by both trusted systems
- When conducted online, replay attacks of cross certification messages are not possible e.g. by including a nonce in the message.

Processes to prove possession of the cross-certification key pair by the requester trusted system, as detailed in 2.1.2 MAY be implemented.

2.6. Dissemination

Certificate dissemination by trusted system MUST be limited to the Subject and to Relying Parties according to the limits expressed by the Subject. CSP disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the CSP's terms and conditions, and any published policy and practice information, to subscribers and relying parties.
Dissemination can be provided in two different ways:

- Online: the subscriber will process request online, on a dedicated CSP web service page.
- Physically: when the subscriber register to a Registration Office.

2.7. Certificate Modification

For some reasons, subscriber may request certificate update due to change to the subject's attributes. The subscriber can, if the CSP offers this service, request a certificate update (e.g rekey) where relevant attributes presented in the certificate have changed. Requests for certificates update issued to a subject who has previously been registered with the same CSP shall be complete, accurate and authorized.

2.8. Certificate Suspension & Revocation

Certificates issued by the CSP may be suspended or revoked.

2.8.1. Certificate Revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

- The CSP SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CSP's Certificate Policy or Certification Practice Statement.
- The CSP SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.
- The CSP SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.
- The CSP SHALL publicly disclose the instructions through a readily accessible online means.
- The maximum delay between receipt of a revocation request and the decision to change its status information being available to all relying parties shall be at most 24 hours.
- The maximum delay between the confirmation of the revocation of a certificate, to become effective and the actual change of the status information of this certificate being made available to relying parties shall be at most 60 minutes.
- For subscriber certificate, The CSP SHALL revoke a Certificate within 24 hours[7].

The CSP may, at its discretion, revoke a certificate when a subscriber fails to comply with obligations set out by its CP, or any subscriber agreement, or any applicable law.

2.8.2. Certificate Suspension

Certificates issued by the CSP may be suspended. CSP has the right to suspend Certificates if it has reasonable doubt that the Certificate contains inaccurate data or Private Key is out of control of its owner and can be used without Subscriber's permission.

The suspension may take place in the following circumstances:

- Explicit request by the Holder of the certificate or by his or her representative (in the case of a Holder that is a legal entity).
- Unauthenticated revocation request (e.g. because the applicant is not able to provide the required confidential code).
- Explicit request by the "interested third party".
- Doubts have arisen regarding the security of the signature device or the confidential data necessary the activation of the key (e.g. PIN, password, OTP).
- Doubts have arisen regarding the correctness of the data contained in the certificate.

CSP should define limits on the suspension period. On expiry of a pre-established time period (normally 60 days) from the suspension date, a suspended certificate is automatically revoked by the CA. Here too the CA sends notification to the Holder of the revocation. This limits on the

[7] If the revocation or suspension request cannot be confirmed within 24 hours then the status needs not be changed

suspension period should be clearly stated on the CSP's CPS. The suspension procedure takes place in the same manner as described for revocation.

2.8.3. Certificate Revocation Management

Certificate Revocation Management services MUST be provided by CSPs as part of the CA services as a core service of the CA.

Certificate Status Change Requests

Certificate Revocation Management service MUST allow end users to request for suspension, release or revocation if one or more of the following occurs:

- The Subscriber requests in writing that the CSP revoke the Certificate.
- The Subscriber notifies the CSP that the original certificate request was not authorized and does not retroactively grant authorization.
- The CSP obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements on this document.
- The CSP obtains evidence that the Certificate was misused.
- The CSP is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use.
- The CSP is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name).
- The CSP is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name.
- The CSP is made aware of a material change in the information contained in the Certificate.
- The CSP is made aware that the Certificate was not issued in accordance with these Requirements or the CSP's Certificate Policy or Certification Practice Statement.
- The CSP determines that any of the information appearing in the Certificate is inaccurate or misleading.
- The CSP's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CSP has made arrangements to continue maintaining the CRL/OCSP Repository.
- The CSP is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate.
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

Requests and reports relating to revocation and/or suspension SHALL be processed in a timely manner.

- The maximum delay between receipt of a revocation or suspension request and the decision to change its status information being available to all relying parties shall be at most 24 hours.
- The maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and the actual change of the status information of this certificate being made available to relying parties shall be at most 60 minutes.

All requests for suspension, reinstating and revocation MUST be suitably authenticated and validated. Once a certificate is definitely revoked (i.e. not suspended) the trusted system MUST ensure that it cannot be reinstated.
Revocation of certificates related to Certificate Signing Keys MUST ONLY be possible under at least dual control. As determined by policy, a Subject's Certificate may be revoked/suspended/ unsuspended by a third party (e.g. employer of a Subject) by sending a suitable request to the CSP, for instigation of a status change.

Certificate status services

Trusted system having obtained a suspension or revocation request via this service, changes the certificate status to either Suspended or Revoked in its Certificate Status Database, and this in turn is used.
A CSP is responsible for updating/providing the status of certificates on the Revocation Status Service Message. Trusted system may implement this using CRL and/or:

- OCSP or CRL shall be supported.
- OCSP should be supported.

If Certificate Revocation Lists (CRLs) concerning end users certificates are used:

- These shall be published at least every 24 hours.
- Every CRL shall state a time for next scheduled CRL issue, unless it is the last CRL issued for those certificates in the scope of the CRL, in which case the **nextUpdate** field in the CRL should be set to "**99991231235959Z**"[8].
- A new CRL may be published before the stated time of the next CRL issue.

If OCSP concerning end users certificates is used:

- The Revocation Status Service MUST be updated when a status change occurs and additionally at least on a daily basis.
- The OCSP shall be as defined in IETF RFC 6960.
- If the OCSP responder receives a request for status of a certificate that has not been issued then the responder shall not respond with a "good" status.

[8] This value, defined in IETF RFC 5280 for certificates that have no well-defined expiration date, is here extended for CRL.

2.9. Certificate Revocation Status

CSP MUST provide access to certificate revocation status service to end users certificates. The CSP shall provide services for checking the status of the certificates. Revocation status information shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CSP, the CSP shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS. The integrity and authenticity of the status information shall be protected. Revocation status information shall include information on the status of certificates at least until the certificate expires.

When both OCSP and CRL are provided:

- Any updates to revocation status shall be available for all methods.
- The information provided by all services shall be consistent over time taking into account different delays in updating the status information for all the methods*.
- The CSP needs to configure OCSP answers for non-issued certificates in a way which is appropriate to meet the consistency requirement (above). In particular, if the responder sends a "revoked" response, the non-issued reason needs to be identifiable (knowing that non-issued certificates do not appear in a CRL).

The revocation status information shall be publicly available.

V. Business Continuity

CSPs MUST have necessary infrastructure and procedures to recover services in case of failure of the Trusted System.

Single point of failure MUST be avoided by replication allowing uninterrupted operations for: dissemination, revocation management services and revocation status services. Availability for these services SHALL not be lower than 99.95%

In case of disaster, CSP MUST ensure they have alternative infrastructure to continue the operations. Trusted systems should have functions that will allow usage of alternative trusted system.

However security risks SHALL always be contained and security issues SHALL never arise during these operations, avoiding risks of key compromise, withdrawing the core security assurance of the trusted system.

The CSP SHALL document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure.

The CSP is not required to publicly disclose its business continuity plans but SHALL make its business continuity plan and security plans available to the CSP-PMA's auditors upon request. The CSP SHALL annually test, review, and update these procedures. The business continuity plan MUST include:

- The conditions for activating the plan.
- Emergency procedures.
- Fallback procedures.
- Resumption procedures.
- A maintenance schedule for the plan.
- Awareness and education requirements.
- The responsibilities of the individuals.
- Recovery time objective (RTO).

- Regular testing of contingency plans.
- The CSP's plan to maintain or restore the CSP's business operations in a timely manner following interruption to or failure of critical business processes.
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location.
- What constitutes an acceptable system outage and recovery time.
- How frequently backup copies of essential business information and software are taken.
- The distance of recovery facilities to the CSP's main site.
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

VI. Key Management Security Controls Requirements

CSPs shall document in detail, within their Certification Practice Statement, how they will meet the technical requirements specified by this standard. The CSP shall ensure sufficient reliability when providing certification services.
Hence key security controls must be in place for each step of the life of a certificate service, comprising of:

- The key generation
- The key storage, backup and recovery
- The public key distribution
- Key escrow
- Key usage and lifecycle

1. Key Management life-cycle

CSPs MUST use cryptographic functions to achieve global security objectives defined. Cryptographic keys will provide assurance for integrity, confidentiality and authentication functions between all the systems involved in the trusted system.
It is essential that throughout the key lifecycle, management of private and secret keys is carried out securely and uses the minimum standards provided in this document.
Certificate signing keys are key pairs generated for producing Certificates and keys for signing certificate status information.

1.1. Key Pair Generation and Installation

All key pairs used in relation with signing or authentication certificates must be generated in and stored in systems meeting the following standards:

- Hardware Security device certified FIPS 140-1 Level 3, FIPS 140-2 Level 3 or Common Criteria (CC) EAL 4 or above.
- Smartcards certified FIPS 140-1 Level 2, FIPS 140-2 Level 2 or CC EAL 3 or above.

The secure cryptographic modules MUST be evaluated and certified to fulfill the following requirements:

- The module MUST ensure the confidentiality and integrity of the keys during their whole life time.
- The module MUST be able to identify and authenticate its users.

- The module MUST restrict access to its services, depending on the user and his role, to those services explicitly assigned to this user and his role.
- The module MUST be able to run a suite of tests to verify that it is operating correctly, and to enter a secure state when it detects an error.
- The module MUST detect attempts of physical tampering and enter a secure state when a tampering attempt is detected.
- The module MUST be able to create audit records for any security-relevant changes.
- The module MAY optionally support backup and restore of keys, but MUST then protect the confidentiality and integrity of the backup data, and require at least dual control for both backup and restore operations.

The CSP's CA SHALL reject a certificate request if the requested Public Key does not meet the requirements set forth in V.2 or if it has a known weak Private Key. Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key without authorization by the Subscriber. If the CSP's CA or any of its designated CSP's RAs generated the Private Key on behalf of the Subscriber, then the CSP's CA SHALL encrypt the Private Key for transport to the Subscriber. If the CSP's CA or any of its designated CSP's RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CSP SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

1.2. Private Key Protection

Private keys shall be securely protected in a hardware device or in software storage as indicated in the previous section. Access to these keys shall be protected with a secret, PIN, biometric control or similar.

The CA private signing key MUST be held within a secure cryptographic device meeting the following requirements:

- FIPS 140-1 Level 3, FIPS 140-2 Level 3.
- Is based on a Trusted system assured to EAL level 4 or higher according to ISO 15408 or equivalent.

When keys are outside the signature creation device, CA private signing keys SHALL be encrypted using a strong security algorithm. The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

1.3. Key Distribution

Private and secret keys MUST NOT be distributed in plain text, as per Private Key Protection. Public keys MUST be kept secure to prevent interception and manipulation until they are distributed.

CSPs MUST have a dedicated key distribution method for the distribution process. A self-signed certificate of a CSP MUST follow these principles listed below:

- The certificate subject and issuer fields MUST be identical.
- The certificate signature MUST be verifiable using data provided within the certificate.

1.4. Key Usage

Private Keys corresponding to CSP CA MUST be limited to sign:

- Certificates for Subscribers
- Cross Certificates.
- Certificates for infrastructure purposes
- CRL
- Certificates for OCSP Response verification.

Authorized key usage MUST only occur within the operational life of the key.

1.5. Key Change

Key Change MUST be carried out securely and MAY be online, or processed physically at the Local RA office.

To carry out properly such process, CSPs MUST have necessary procedure to handle such case.

1.6. Key Backup and Recovery

The CSP's CA Private Key SHALL be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. The only keys that can be requiring backup are subscriber encryption keys. As long as the CSP securely backs up users decryption keys, security is not compromised. However, signing keys have different requirements from decryption keys. In fact, as the next section describes, backing up signing keys destroys a basic requirement of a PKI (Except).

1.7. Key Archival

Systems SHALL NOT allow archiving of signing private keys. Public keys archival is allowed for the purpose of verification of electronic signatures.

1.8. Key Destruction

When signing keys reach the end of life, keys MUST be destroyed, so signing keys cannot be retrieved. Systems reaching end of life that have been used for the entire key life cycle MUST follow a proper data wiping procedure, where keys (private or public) associated with it MUST be destroyed as well.

Trusted systems SHALL provide the capability to wipe plaintext secret and private keys stored in both hardware and software.

2. Key Sizes

Certificates MUST meet the following requirements for algorithm type and key size:

Subscriber Certificate	
Hash algorithm	SHA-256, SHA-384, SHA-512, SHA-512/256 SHA3-256, SHA3-384, SHA3-512
Minimum RSA modulus size (bits)	2048
ECC curve[9]	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048, N= 256
Validity Period	No greater than 825 days.

3. Key Escrow

Key escrow means that a third party (such as law enforcement) can obtain the decryption keys required to access encrypted information, this requires a legal process, as risks of unauthorized access to sensitive or personal data is high.

This is different from key backup and recovery requirements, focusing on commercial needs that exist regardless of law enforcement requirements.

Key escrow is required/allowed as per the law enforcement and legal court proceedings.

However:

- The CA shall not hold the subject private signing keys in a way which provides a backup decryption capability (commonly called key escrow), and results in its use not being under the sole control (or if the subject is a legal person "control") of the signer or owner[10].
- If the subject's private key is to be used for authentication, then the CA should not hold the subject's private signing keys in a way which provides a backup decryption capability (commonly called key escrow), and results in its use not being under the control of the signer or owner.
- If the CA requires a subject private key used for decryption to be escrowed by the CA or a designated entity, then this private key shall not have other key usages.

4. SCD Security

The signature creation devices MUST follow the same security requirements as the key component of the PKI as those listed in chapter 4 before.

SCD must be conform to FIPS 140-1 Level 3 or EAL4 level of assurance. Access or use of the SCD MUST be strictly controlled, the CSP operating the trusted system MUST not be able to misuse it.

Initialization and preparation of SCD MUST be carefully handled and prior to acquiring to a vendor, the CSP MUST ensure that SCD is genuine from a certified vendor.

[9] Others agreed elliptic curve family

Curve family	Short curve name	References
FR	FRP256v1	ANSSI
Brainpool	brainpoolP256r1 brainpoolP384r1 brainpoolP512r1	IETF RFC 5639 [5]

[10] This does not preclude the CSP generating and managing the key on behalf of the user provided that the key is kept under the sole control (or if the subject is a legal person "control") of the user.

The initialization, formatting and file structure creation MUST use secure values, parameters and access control conditions, leaving the SCD in a secure configuration, which cannot be misused at any time.
Where the key pair is generated outside the SCD, the cryptographic module generating the key pairs MUST be evaluated and comply with the following requirements:

- The module MUST ensure the confidentiality and integrity of the keys so long as they are under the control of the module:
- The module MUST ensure the confidentially of private keys transferred from the module to a SCD.
- The module MUST ensure the integrity of public keys exported to other systems or applications.
- The module MUST be able to identify and authenticate its users.
- The module MUST restrict access to its services.

5. Other Optional services

Depending on the service provided by CSPs in Qatar, additional secure services might be provided to Subjects, carrying the same constraints and level of security described above on previous chapters.

5.1. Time stamping services

A Time-Stamping Authority [TSA] is a third party trusted to provide time-stamping services, i.e. generate timestamp tokens, which can serve as evidence that a data item existed before a certain point in time (proof of existence).

The TSA MAY control the origin of each request before checking its correctness. A solution to perform such a control could be to make use of a data origin authentication mechanism.

The TSA SHALL verify that the request for time-stamping uses a hash algorithm that is specified as approved by hashing method based on TDES or equivalent level. A CSP SHALL document and implement a dedicated TSA policy to manage a TSA effectively. The TSA service SHALL be governed by the policy.

A CSP providing time-stamping services to the public, is called the Time-Stamping Authority (TSA). The TSA has overall responsibility for the provision of the time-stamping services. The TSA has responsibility for the operation of one or more TSUs (time-stamping unit) which creates and signs on behalf of the TSA. The TSA responsible for issuing a time-stamp is identifiable. In addition, the following requirements apply:

- The TSA shall have a system or systems for quality and information security management appropriate for the time-stamping services it is providing.
- The generation of the TSU's signing key(s) shall be undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control. The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practices.

5.1.1. Time Parameter Generation

The TSA's trusted time source(s) MUST be synchronized to Co-ordinated Universal Time (UTC) within the tolerance dictated by policy (e.g. to within 1 second)
The TSA's clock SHALL be synchronized with UTC using a mechanism that is highly reliable.

5.1.2. Time-Stamping Unit Generation

A TSU certificate contains a TSU public key and is signed by a CA private key. The following particular requirements apply:

- The generation of the TSU's signing key(s) shall be undertaken in a physically secured environment by personnel in trusted roles under, at least, dual control. The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practices.
- The generation of the TSU's signing key(s) shall be carried out within a cryptographic module(s) which meets the requirements in V.1.1.
- The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key shall be recognized. The following requirements apply:

TSU certificates	Issuers of TSU certificates	Users of TSU certificates
TSU public key	• shall support RSA with SHA256 or SHA-512 • should support EC-DSA with SHA-256	• shall support RSA with SHA256 or SHA-512 • should support EC-DSA with SHA-256
Issuer CA public keys	• shall support RSA with SHA256 or SHA-512 • should support EC-DSA with SHA-256	• shall support RSA with SHA256 or SHA-512 • should support EC-DSA with SHA-256

6. Auditing

All components for CSP operations MUST allow auditing operations by CSP-PMA's auditors, Log generation of all security events of all components of the CSP MUST exist and process for reviewing, monitoring and auditing operations by CSP-PMA's auditors.

Any attempt to interfere with the PKI process by a CSP on any component would constitute a breach of the principle itself of a PKI. Auditing on systems MUST remain activated and allow traceability of security events or system related events.

References

- **CEN TS 419 261**: "Security requirements for trustworthy systems managing certificates and time stamps".
- **ETSI TS 101 533-1**: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".
- **ETSI TS 102 042**: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".
- **ETSI TS 119 312**: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
- **ETSI TS 119 612**: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".
- **ETSI EN 319 403**: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".
- **ETSI EN 319 411-2**: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
- **ETSI EN 319 421**: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
- **IETF RFC 3647**: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".
- **IETF RFC 5246**: "The Transport Layer Security Protocol Version 1.2".
- **ISO/IEC 7498-2**/Recommendation ITU-T X.800: "Data communications network - Open systems interconnection - Security, structure and applications: Security architecture for open systems interconnection for CCITT applications". ETSI 9 ETSI EN 319 411-1 V1.2.2 (2018-04).
- **ISO 19005 (parts 1 to 3)**: "Document management - electronic document file format for long-term preservation".
- **ISO/IEC 27002:2013**: "Information technology - Security techniques - Code of practice for information security management".

APPENDIX A

Certificate Profile

The issuing CA SHALL meet the technical requirements set forth in Section III (CP and CPS) and Section V.2 (Key Sizes). Issuing CAs SHALL generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.
The Certificate is a SEQUENCE of three **required** fields. These fields are described in detail in the following tables:

1. TBSCertificate Field

Field	Description	Attributes
TBSCertificate	The sequence TBSCertificate contains information associated with the subject of the certificate and the CA that issued it.	**version** **serialNumber** **signature** **issuer** **validity** **subject** **subjectPublicKeyInfo** **UniqueIdentifier** **extensions**

1.1. Certificates issued to natural persons

- **Basic Certificate Fields**

Attribute	Field	Value
version		
		Certificates MUST be of type X.509 v3
serialNumber		
		Validated for duplicates
signature		
		This field contains the algorithm identifier for the algorithm used by the CA to sign the certificate. This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence Certificate.
issuer		
	When the issuer is a legal person, the identity of issuer shall contain at least the following attributes.	
	countryName	As specified in CSP license
	commonName	As specified in CSP license
	organisationName	As specified in CSP license
validity		
	NotBefore	Certificate generation date/time
	NotAfter	No greater than 825 days.
subject		
	The subject field shall include the following attributes	

	countryName		QA
	Choice of	**givenName** and **surname**	
	Or	**pseudonym**	Shall not be present if the **givenName** and **surname** attribute are present.
	commonName		Shall contain a name of the subject as per Qatari ID.
	If these mandatory attributes are not sufficient to ensure Subject name uniqueness within the context of the issuer the **serialNumber** shall be present.		
	serialNumber		Has no defined semantics beyond ensuring uniqueness of subject names. It may contain a number or code assigned by the CA or an identifier assigned by a government or civil authority (Subject's Qatar ID)
	Additional attributes other than those listed above may be present		
	organizationName		
	organizationIdentifier		
SubjectPublicKeyInfo			
	Algorithm		The subject public key should be selected according to Electronic Signature Algorithms Standard.
	subjectPublicKey		

- **Standard certificate extensions**

Extension	Field	Critical	Value
AuthorityKeyIdentifier			
	keyIdentifier		The authority key identifier extension shall be present, containing a key identifier for the issuing CA's public key. Two common methods for generating key identifiers from the public key are: • The **keyIdentifier** is composed of the 160-bit SHA-1 hash of the value of the BIT STRING **subjectPublicKey** (excluding the tag, length, and number of unused bits. • The **keyIdentifier** is composed of a four-bit

			type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING **subjectPublicKey** (excluding the tag, length, and number of unused bits).
AuthorityInfoAccess			
	When the issuing CA is not represented by a self-signed root certificate, the Authority Information Access extension shall include		
	AccessMethod		**AccesMethod** OID = **id-ad-caIssuers** OID
	Accesslocation		Specifying at least one access location of a valid CA certificate of the issuing CA. At least one access location shall use the http or https scheme.
	When OCSP is supported by the issuing CA, the Authority Information Access extension shall include		
	AccessMethod		**AccesMethod** OID = **id-ad-ocsp** OID
	Accesslocation		Specifying at least one access location of an OCSP responder authoritative to provide certificate status information for the present certificate. In such case, at least one access location shall specify either the http or the https scheme. Such access location shall reference a publicly available OCSP responder, which accepts unsigned and unauthenticated status requests.
keyUsage			
	The **keyUsage** extension shall be present.		

			shall contain one (and only one) of the key usage settings: • **digitalSignature**: Use when the public key is used with a digital signature mechanism to support security services other than non-repudiation, certificate signing, or CRL signing. A digital signature is often used for entity authentication and data origin authentication with integrity. • **nonRepudiation**: Use when the public key is used to verify digital signatures used to provide a non-repudiation service. Non-repudiation protects against the signing entity falsely denying some action (excluding certificate or CRL signing). • **keyEncipherment**: Use when a certificate will be used with a protocol that encrypts keys. An example is S/MIME enveloping, where a fast (symmetric) key is encrypted with the public key from the certificate. SSL protocol also performs key encipherment. • **dataEncipherment**: Use when the public key

			is used for encrypting user data, other than cryptographic keys. • **keyAgreement**: Use when the sender and receiver of the public key need to derive the key without using encryption. This key can then can be used to encrypt messages between the sender and receiver. Key agreement is typically used with Diffie-Hellman ciphers. • **keyCertSign**: Use when the subject public key is used to verify a signature on certificates. This extension can be used only in CA certificates. • **cRLSign**: Use when the subject public key is to verify a signature on revocation information, such as a CRL. • **encipherOnly**: Use only when key agreement is also enabled. This enables the public key to be used only for enciphering data while performing key agreement. • **decipherOnly**: Use only when key agreement is also enabled. This enables the public key to be used only for

			deciphering data while performing key agreement.
cRLDistributionPoint			
	The CRL distribution points extension identifies how CRL information is obtained. This extension **MAY be present**. If present, it **MUST NOT be marked critical**. The **cRLDistributionPoints** extension is a SEQUENCE of:		
	distributionpoint		shall include at least one reference to a publicly available CRL. At least one of the present references shall use either http (http://) or ldap (ldap://) scheme.
subjectAltName			
	This extension **SHALL not be marked critical**. The **subjectAltName** extension allows identities to be bound to the subject of the certificate. The sequence MUST contain at least one entry.		
	otherName		
	rfc822Name		Electronic mail address
	dNSName		domain name system
	x400Address		Originator/Recipient (OR) address
	ediPartyName		EDIPartyName
	directoryName		Name
	uniformResourceIdentifier		URI
	iPAddress		iPAddress name forms.
	registeredID		OID
subjectKeyIdentifier			
	This extension **MUST appear** To facilitate certification path construction.		
	keyIdentifier		the value of the subject key identifier MUST be the value placed in the key identifier field of the authority key identifier extension of certificates issued by the subject of this certificate.

certificatePolicies			
	This extension **should not be marked critical**. The **certificatePolicies** extension shall be present and shall contain the identifier of at least one certificate policy which reflects the practices and procedures undertaken by the CA.		
	policyIdentifier		**Required** Indicating a Certificate Policy OID.
	policyQualifiers		**Recommended** Id-qt-cps
	cPSuri		**Optional** contains a pointer to a Certification Practice Statement (CPS) published by the CA.

1.2. Certificates issued to legal entities

All certificate fields and extensions shall comply with requirements defined for certificate issued to natural person with the amendments specified below concerning **subject** attribute.

Attribute	Field	Value
subject		
	The subject field **shall include** at least the following attributes. Only one instance of each of these attributes **shall be present**. Additional attributes may be present.	
	countryName	QA
	organizationName	Shall contain the full registered name of the subject (legal person).
	organizationIdentifier	Shall contain an identification of the subject organization different from the organization name.
	commonName	Shall contain a name commonly used by the subject to represent itself. This name needs not be an exact match of the fully registered organization name.

2. signatureAlgorithm

The signatureAlgorithm field contains the identifier for the cryptographic algorithm used by the CA to sign this certificate. "Electronic Signature Algorithms Standard" list supported and recommended signature algorithms.
This field MUST contain the same algorithm identifier as the signature field in the sequence **tbsCertificate.**

3. signatureValue

The **signatureValue** field contains a digital signature computed upon the **ASN.1 DER** encoded **tbsCertificate**. This signature value is encoded as a **BIT STRING** and included in the signature field. By generating this signature, a CA certifies the validity of the information in the tbsCertificate field. In particular, the CA certifies the binding between the public key material and the subject of the certificate.

APPENDIX B

CRL Profile

The CRL shall be as defined in **RFC 5280**. CRL consist on **CertificateList**, a sequence of three required fields, that is described in detail in the following table:

Field	Description	Value
tbsCertList	This field is itself a sequence containing the name of the issuer, issue date, issue date of the next list, the optional list of revoked certificates, and optional CRL extensions. When there are no revoked certificates, the revoked certificates list is absent.	**version** **signature** **issuer** **thisUpdate** **nextUpdate** **revokedCertificates** **crlExtensions**
signatureAlgorithm	The signatureAlgorithm field contains the algorithm identifier for the algorithm used by the CRL issuer to sign the **CertificateList**. The field is of type **AlgorithmIdentifier**. This field **MUST** contain the same algorithm identifier as the signature field in the sequence **tbsCertList.**	**AlgorithmIdentifier**
signatureValue	The **signatureValue** field contains a digital signature computed upon the ASN.1 DER encoded **tbsCertList**.	This signature value is encoded as a BIT STRING and included in the CRL **signatureValue** field.

TBSCertList, is a sequence of required and optional fields. The required fields identify the CRL issuer, the algorithm used to sign the CRL, and the date and time the CRL was issued. Optional fields include the date and time by which the CRL issuer will issue the next CRL, lists of revoked certificates, and CRL extensions. This field is described as follow:

Field	Description and Nature	Value
Version	**Optional** field describes the version of the encoded CRL.	When extensions are used, as required by this profile, this field MUST be present and MUST specify version 2.
signature	**Required** field contains the algorithm identifier for the algorithm used to sign the CRL.	This field MUST contain the same algorithm identifier as the **signatureAlgorithm** field in the sequence **CertificateList**.

issuer	**Required** field identifies the entity that has signed and issued the CRL. The issuer identity is carried in the issuer field.	The issuer field MUST contain a non-empty **X.500** distinguished name (DN). The issuer field is defined as the **X.501** type Name, and MUST follow the encoding rules for the issuer name field in the certificate.
thisUpdate	**Required** field indicates the issue date of this CRL.	CRL issuers conforming to this profile MUST encode **thisUpdate** as **UTCTime**.
nextUpdate	**Optional** field indicates the date by which the next CRL will be issued.	CRL issuers conforming to this profile MUST encode **nextUpdate** as **UTCTime**. **Note**: CRL issuers SHOULD issue CRLs with a **nextUpdate** time equal to or later than all previous CRLs.
revokedCertificates	The revoked certificate list is **optional** to support the case where a CA has not revoked any unexpired certificates that it has issued.	When there are no revoked certificates, the revoked certificates list MUST be absent. Otherwise, revoked certificates are listed by their serial numbers.
crlExtensions	This field may only appear if the version is 2. If present, this field is a sequence of one or more CRL extensions.	**AuthorityKeyIdentifier** **IssuerAltName** **CRLNumber** **deltaCRLIndicator** **IssuingDistributionPoint** **FreshestCRL** **authorityInfoAccess**

APPENDIX C

Particular Requirements

1. CRLs

A CRL is signed by a CRL Issuer. Particular cryptographic algorithms shall apply to CRL Issuer public keys with the amendments defined in the below table:

CRLs	Issuers of CRLs	Users of CRLs
CRL issuer keys	**Shall** support RSA with SHA-256.	**Shall** support RSA with SHA-256 or SHA-512. **Shall** support EC-DSA with SHA-256.

2. OCSP responses

An OCSP response is signed by an OCSP responder. These requirements, described on the table, shall apply to the hash algorithm and the signature algorithm used by OCSP responders.

OCSP response	Issuers of OCSP responses	Users of OCSP response
OCSP responder keys	**Shall** support SHA-256 with RSA.	**Shall** support RSA with SHA-256 or SHA-512. **Shall** support EC-DSA with SHA-256.