Adobe Approved Trust List

Technical Requirements

Version 2.0

June 2017

Summary

The Adobe Approved Trust List (AATL) is a program that allows millions of users around the world to create digital signatures that are trusted whenever the signed document is opened in Adobe® Acrobat® or Acrobat® Reader® software. Essentially, both Acrobat and Reader have been programmed to reach out to a web page to periodically download a list of trusted digital certificates. Any digital signature created with a credential that can trace a relationship ("chain") back to the trustworthy certificates on this list, for an approved certificate issuance policy, will display as trusted by Acrobat and Reader. This certificate can also be considered as providing a high-assurance proof of the identity of the signer.

> *Note: such trusted digital signatures can support signatures created by natural or legal persons, or applications or devices, e.g. electronic signatures or electronic seals such as defined in some Regulations like eIDAS (the European Regulation on Trust Services).*

For the purpose of its inclusion in the AATL, a Member may submit to Adobe either the certificate of the CA issuing the signers' certificates (the Issuing Certification Authority (ICA)), or the certificate of an upper level CA or a Root-CA (noted RCA) in which cases, additional requirements must be fulfilled.

The **general requirements** are described in the paragraphs identified with the prefix "**G**". They may relate to the ICA, the upper CAs (RCA), or the Member as the legal entity in charge of the submitted certificate. Where relevant, the target entity is specified.

The **technical requirements** listed in this document cover:

(a) The requirements for end-entity certificates, e.g. the signers' certificates and the related certificate policy(ies), identified by "**EE**",

(b) The requirements for the issuing CA, identified by "**ICA**", and, when relevant,

(c) The requirements for the upper level CA(s) or Root-CA under which one or more ICAs are certified, identified by "**RCA**".

In this document, the terms "*all the (I)CA that inherit trust from a RCA by virtue of the AATL*" do not necessarily cover all the (I)CA (and their certificates) that inherit trust from an upper or Root CA, but only these that fulfil the AATL requirements and have been explicitly recognized by Adobe under a contractual agreement with the corresponding Member.

General requirements

G1

The Member must be the legal entity having final liability and responsibility on the ICA, or on the upper level or Root CA and all the (I)CAs that inherit trust from such CA by virtue of the AATL, and on the related services for the issuance of end-entity certificates, whether sub-contracted or not.

G2

The ICA, or the upper level or Root CA and all the (I)CAs that inherit trust from that upper or Root CA by virtue of the AATL, must have successfully passed within the past 24 months, and continue to pass at least on a 2-years basis, an audit.

The audit aims to prove that the Member implements what is stated in its documentation, in particular the CPS (Certificate Practice Statements) and CP (Certificate Policies), and that it achieves the level of security specified by the audit scheme.

The audit also helps to support the vetting by Adobe that the Member conforms to the present AATL requirements, as further described in **G6(c)**, (for this purpose, the scope of the audit may be extended to the AATL requirements, to provide the evidence that the Member fulfills the present AATL requirements).

In all cases the scope of the audit must encompass:

- The overall operations of the CA (network, physical protection, HR and other general functions management);
- The registration services;
- The revocation management services;
- The dissemination / publication services;
- The revocation status information services;
- The subject device provisioning services;
- The certificate generation services.

The following audit schemes are recognized by Adobe:

(a) ETSI EN 319 411-1 NCP (ETSI TS 102 042 is accepted until 31 December 2017);

(b) ETSI EN 319 411-2 QCP-n or QCP-l (ETSI TS 101 456 accepted until 31 December 2017);

(c) WebTrust for CA v.2.0 or later;

(d) ISO 21188:2006.

If a Government Member is required to use a different internal audit scheme, or if a Member adopts another scheme not recognized by Adobe, it may use such scheme provided that the audit consists of comparable criteria that are available for public review, and provided that the audit is performed by a Qualified Auditor (e.g. conforming to **G3** below). Adobe reserves the right to request additional proof and documentation to assess the adequacy of the scheme. If such assessment requires substantial work or resources, the related costs might be at the charge of the Member.

In case of non-conformities, the Member must provide Adobe with evidences of implementation of mitigation measures and compensation controls for evaluation and approval by Adobe at its sole discretion. Adobe may require the Member to remedy any failure to fulfill the AATL requirements and where the Member does not act accordingly, if applicable within a time limit set by Adobe, Adobe may remove the concerned ICA or RCA of the Member from the AATL program.

As an alternative to the presentation of a conformity assessment report confirming the conformity against one or more of the above listed audit schemes specifications, demonstrating compliance with the AATL requirement can be achieved when the submitted ICA or RCA:

(e) meets the Medium Hardware Assurance Requirements of the US Federal Bridge (see https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000SfwQ), the SAFE-BioPharma bridge, or the CertiPath commercial bridge, by privilege of having the Supplied Certificate cross-certified to the bridge; or

(f) is listed and granted a CA/QC qualified status in one of the European Member State national Trusted Lists (EUTL) as a qualified trust service for the issuance of qualified certificates for electronic signatures or electronic seals and the trusted list indicates directly, or indirectly though the certificate, that the certificate is stored on a Qualified Signature Creation Device.

G3

Conformity assessment bodies that will carry out assessments against the standards or specifications referred to in **G2** must be independent from the Member's organization and must be formally accredited or recognized for the applicable scheme. In particular:

(a) the auditor conducting ETSI audits must be accredited against ISO/IEC 17065 and ETSI EN 319 403 for audits against ETSI EN 319 411 standards series;

(b) the auditor conducting WebTrust audits must be a WebTrust licensed Practitioner for WebTrust audits;

(c) the auditor conducting ISO 21188 audits must be accredited against ISO/IEC 17065 for ISO 21188 audits.

G4

The Member must make any applicable Audit Report available to Adobe no later than three months after the end of the audit period. In the event of a delay greater than three months, the Member must provide an explanatory letter signed by the Qualified Auditor.

G5

The Member must ensure that the ICA, or the upper level or root CA and all the (I)CAs that inherit trust from that upper level or root CA by virtue of the AATL, meets the technical requirements for the whole duration of the Membership Agreement.

G6

The Member must provide written evidences to support demonstration of conformity with all the applicable technical requirements of the AATL program:

(a) The Member must provide a self-assessment containing evidences to support demonstration of conformity with all the applicable requirements; and,

(b) The Member must disclose to Adobe its Certification Practice Statement (CPS) and relevant Certificate Policies (CP). The CPS or CP must include all the material required by RFC 3647, and must be structured in accordance with RFC 3647.

Note: The Member must publicly disclose its business practices to the extent required by the Member's selected audit scheme. The Member is encouraged to provide any other information it deems appropriate to demonstrate the conformity with the applicable requirements.

(c) The audit report also provides evidences for certain AATL requirements. The Member is invited to point the sections of the audit report that addresses these requirements where relevant. If the audit shows non-conformities for the related requirement(s) Adobe reserves the right to assess the conformity through the documentation provided by the Member.

Adobe reserves the right to request additional proof and documentation at any time.

G7

The Member must notify Adobe immediately (unless otherwise restricted by law enforcement agencies or governmental authorities) of any breach of security or loss of integrity, CA (private key) compromise, personal data protection breach, security issues that lead to certificate miss-issuance, or suspicion thereof, on any server, PC or other system or endpoint that is logically connected to certificate issuance and management systems. Notifications can be sent via email to AATLNotification@adobe.com or to any other email address duly provided by Adobe.

G8

With regards to **G7**, the Member must provide Adobe with details about the notified breach and about remediation / action plan within 3 days after the notification.

G9

The Member must notify Adobe, at least 1 month in advance, of any change in the provision of the submitted ICA/RCA services regarding the PKI hierarchy, the applicable certification practices statement and the applicable certificate policies. In particular:

(a) The addition of a new (I)CA under a submitted upper level or root CA.

(b) The addition of a new certificate policy under a submitted ICA / upper level or root CA.

(c) Changes regarding certificate issuance procedures, including registration, issuance of devices where end-entity private key resides and revocation procedures.

(d) Termination or hand-over of ICA and/or upper level or root CA services.

G10

Adobe reserves the right not to accept a candidate Member's ICA / upper level or root CA and to remove a Member's ICA / upper level or root CA from the AATL at its sole discretion. Adobe may notify the concerned Member of the reasons for such a decision. Those reasons may include but may not be limited to:

(a) audit with major non-conformities not acceptable by Adobe (e.g. with no satisfactory resolution or mitigation plan);

(b) failure to notify a change for which a prior notification is required under **G9**;

(c) failure to notify a security breach;

(d) failure to remedy a security breach;

(e) failure to remedy any failure to fulfill AATL requirements, if applicable within a time limit set by Adobe.

G11

Existing Members of the AATL program must migrate to the present version of the AATL requirements and ensure that all their ICAs and RCAs listed in the AATL comply with it.

Adobe reserves the right to remove any non-compliant ICAs, upper level CAs or root CAs from the AATL program.

G12

Cross-certification and root-signing initiated by an ICA or RCA listed in the AATL is allowed under the AATL program but must not automatically result in a transfer of AATL rights to the cross-certified or root-signed entity. Adobe reserves the right to impose technical measures to enforce this general requirement. See also requirement **RCA1**.

Requirements for End-entity certificates

EE1

All end-entity certificates issued by ICA or RCA must be X.509 v.3 certificates, profiled as per RFC 5280.

EE2

All end-entity certificates should contain a combination of KeyUsage and ExtendedKeyUsage extensions, as defined in RFC 5280, which are valid for digital signature use in Adobe Acrobat and Acrobat Reader. Adobe provides a list of supported extension requirements at this web page: http://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/changes.html.

EE3

The Member is not required to add any custom OIDs to their certificates as part of the AATL. However, Member can consider adding appropriate Adobe-specific OIDs to new certificates to allow for automatic time stamping (RFC3161 as updated by RFC 5816) and revocation information embedding within Adobe products for long-term validation purposes as described at this web page: http://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/oids.html#x-509-extension-oids

When a Time Stamping Authority is imposed or recommended to the signers by the Member, it must follow state of the art security policies and provide proper timestamps. The time-stamping practices and policies must be provided to Adobe and Adobe reserve the right to not accept the Time Stamping Authority.

EE4

All end-entity key pairs must:

(a) be generated:

1) either by using a trustworthy system, taking all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key, and then securely transferred in a secure cryptographic hardware device conform to (c) below, or,

2) directly generated by and stored in such a secure cryptographic hardware device.

(b) have key length and algorithm susceptible to remain valid for the lifetime of the certificate, as recommended by authoritative researchers in the field of cryptography.

Note: Authoritative researchers includes NIST, ETSI, IETF, BSI, ANSSI, IAD-NSA, national authorities, academic institutions, research centers and others. For example, the ETSI TS 119 312 specification and *other PKI industry studies provide guidance for the selection of key lengths and signature algorithms susceptible to remain valid for a certain amount of time.*

For RSA signature technology, a key length of 2048-bit or higher is required for EE certificates that have been issued on or after 1 July 2013.

For Elliptic Curve signature technology, a key length of 256-bit or higher is required for EE certificates that have been issued on or after 1 July 2013.

The use of SHA256 hash algorithm or stronger is required for ICA certificates. The use of SHA1 hash algorithm is only allowed for EE certificates that have been issued before 1 July 2013.

(c) be stored in a secure cryptographic hardware device that:

1) is certified:

  i. FIPS 140-2 Level 2; or

  ii. Common Criteria (ISO 15408 & ISO 18045) - Protection Profiles CEN prEN 14169 (all parts applicable to the device type) or standards such as CEN EN 419 241 series or equivalent, for remotely managed devices; or

  iii. by an EU Member State as a Qualified Signature Creation Device (QSCD) after 1 July 2016, or that was recognized as a Secure Signature Creation Device (SSCD) by an EU Member State designated body before 1 July 2016.

2) is controlled by the signer (or by the subscriber if the signer is not a physical person):

  i. either directly, by possession (after secure hand-over to the subscriber when applicable). In this case:

    1. the activation of the private key must require the signer's authentication;

    2. the device must prevent exportation or duplication of the private key.

  ii. or via a third party managing the secure cryptographic hardware device on behalf of the signer. In this case:

    1. the key activation must rely on at least a 2-factor authentication (2FA) process;

    2. no duplication of the private key is allowed, except for duly documented service availability purpose, and the duplicated key must abide at least the same security measures as the original;

    3. the third party must disclose to Adobe the documentation (technical, procedural and operational) on the management of the secure cryptographic hardware device;

    4. the third party agrees on an annual verification of the conformity of the service with its Practice Statement, or must be certified against standards like the CEN EN 419 241 series listed above or equivalent.

EE5

The Member must provide Adobe with sample end-entity certificates and sample signed PDF documents in order to check the compatibility with the AATL requirements prior to the official publication in the List.

Requirements for Issuing CA certificates

ICA1

If only some of the certificates issued by the ICA are compliant with the **EE** requirements, then:

(a) the Member must be able to differentiate those certificates through the submission to Adobe of specific certificate policy OID values. Only the certificates marked by these certificate policy OID values will be deemed as valid by Adobe Acrobat and Acrobat Reader software.

(b) if the ICA issues other CA's certificates, it must also fulfill the **RCA** requirements.

ICA2

The submitted ICA certificate must be a X.509 V.3 certificate, profiled as per RFC 5280.

ICA3

The ICA Certificate Subject Name must contain an 'organizationName' attribute (as specified in Recommendation ITU-T X.520) having as value the full registered name of the Member (as notified to Adobe) and, where applicable, an 'organizationIdentifier' attribute (as specified in Recommendation ITU-T X.520) having as value the registration number of the Member as stated in the official records.

ICA4

The Member must be generating and protecting key pair(s) for the supplied ICA Certificate(s) in a medium that prohibits exportation and duplication that could allow unauthorized use of the private or secret keys.

A hardware security module that meet FIPS 140-2 Level 3 or equivalent provides a suitable medium.

ICA5

With regards to the submitted ICA(s), the Member must demonstrate the use of strong subscriber/subject identification and authorization procedures including during certification application and secure delivery of end-entity secure hardware device when applicable.

In particular:

(a) The ICA warrants that all information and representations made by the Subscriber are true. For this purpose, the applicant registration process must rely on a strong identity proofing, based on a face to face meeting with the subscriber, or on a procedure that provides an equivalent assurance (e.g. by means of a secure video communication).

(b) In application of **G1** above, the ICA must assume full responsibility for RA activities, especially when delegated to external/third-party organizations.

(c) The applicant registration process must ensure that certificate generation is never performed before the registration approval. In particular, it must:

1) Complete the identity verification before the certificate generation, to prevent that certificates are:

i. generated based on identity information that is only supposed to be valid;

ii. used before a complete identity verification is really performed;

2) Mandate confirmation from the subscriber that the information to be certified is correct before the certificate application is approved;

3) Mandate that the certificate application shall be approved by the Registration Authority (RA) before sending the certificate request to the certificate generation service.

(d) When the subscriber is not the subject of the certificate, evidences on the link with the subject must be provided. In particular:

1) When the subject is an organization, the subscriber must provide evidences of association with, and proofs of entitlement to represent, that organization.

2) When the subject is an employee of, or is associated to, an organization represented by the subscriber, or if the subject is a natural person represented by another person (e.g. the subscriber), the subject must mark his/her consent on the certification request.

3) When the subject is a DNS, a system, a device or an application, the subscriber must proof ownership or rights on that DNS, system, device or application.

(e) The procedure(s) to hand-over a secure device, or to deliver key activation data, must ensure that the recipient is the authorized subscriber, amongst other by reconciliation with the registration information.

ICA6

The Member ICA must demonstrate any of the following conditions:

(a) A robust capability to revoke certificates immediately upon any actual or suspected loss, disclosure or other compromise of the subscriber's private key when reported lost, when there is a security or integrity problem, or when any certified information or information related to the certificate application file has been changed. The Member must be willing to provide documentation to Adobe on the underlying processes and procedures.

(b) The short-lifetime, limited applicability or specific handling and management of the private key and/or of the certificate do not require a revocation service as the Member guarantees that the certificate was valid at any time of use and the corresponding private key was under control of use by the subject of the certificate. In this case the Member must be willing to provide necessary documentation to Adobe on the underlying processes and procedures to determine, at Adobe's sole discretion, their equivalence to the security offered by a revocation service.

ICA7

With regards to **ICA6**, whatever revocation facilities is implemented, if any, all issued certificates must include information about, or information that can be used to enquire about, the validity status of the certificate.

(a) When implementing **ICA6.(a)**, at least one of OCSP or CRL must be supported and the end-entity certificates must bear the related information to enquire about the revocation status of the certificate (AIA or CDP extensions);

(b) When implementing **ICA6.(b)**, in the absence of a standardized statement the Member must issue such certificate under a specific dedicated certificate policy OID included in the certificate and notify such OID to Adobe.

ICA8

The Member ICA must demonstrate capability to have its own certificate revoked in case of security compromise or, for self-signed certificates, to notify Adobe of such comprise immediately. When implementing revocation facilities, the information to enquire about the revocation status of the ICA certificate (AIA or CDP extensions) must be present in the ICA certificate, otherwise, the Member must agree with Adobe on an incident management plan so that Adobe can swiftly remove the compromised certificate form the AATL.

ICA9

The ICA must have key length and algorithm susceptible to remain valid for the lifetime of the certificate, as recommended by authoritative researchers in the field of cryptography.

> *Note: Authoritative researchers includes NIST, ETSI, IETF, BSI, ANSSI, IAD-NSA, national authorities, academic institutions, research centers and others. For example, the ETSI TS 119 312 specification and other PKI industry studies provide guidance for the selection of key lengths and signature algorithms susceptible to remain valid for a certain amount of time.*

For RSA signature technology, a key length of 2048-bit or higher is required for ICA certificates.

For Elliptic Curve signature technology, a key length of 256-bit or higher is required for ICA certificates.

The use of SHA256 hash algorithm or stronger is required for ICA certificates. The use of SHA1 hash algorithm is only allowed for ICA certificates that have been issued before 1 July 2013.

ICA10

Certificate Authority Security Controls. Members must meet all the sub-parts below:

(a) Member must provide evidence of appropriate network security controls, including IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) systems, as well as evidence of the segmentation of its key certificate issuance systems from non-related servers and systems such as marketing websites, etc.

(b) Member must have in place an incident response plan to respond to compromise or breach of its online systems as well as its certificate issuance systems.

(c) Member must demonstrate it has controls in place to prevent unauthorized or illegitimate software from executing within its systems, including but not limited to anti-virus and anti-malware software.

(d) Member must provide evidence that system administrators in Member's network do not have access to certificate issuance systems due to proper segmentation of duties and least privilege principles.

(e) Member must provide evidence of security controls in place for all accounts with certificate issuance rights.

(f) Member must provide evidence of the adoption of not only vulnerability assessment testing, including but not limited to penetration testing and application scanning (in both a credentialed and un-credentialed state), but also corrective action based on any negative results. Member should not have any common security vulnerabilities (see Common

Weakness Enumeration (CWE) and Open Web Application Security Project (OWASP)) on public facing or RA / partner web sites.

(g) Member must demonstrate robust logging procedures, including aggregation of logs at alternate sites, tamper-evidence controls, and monitoring schedules.

(h) Member must provide evidences on good practices and details on its internal auditing / log monitoring practices in regards to certificate issuance (e.g. how often is Member checking certificate inventory against expected inventory?), particularly when it comes to signing certificates.

(i) Member must provide evidences on good practices and details on certificate issuance processes, to include RA and user authentication practices (as distinct from ICA5 above for subscriber/subject identification).

(j) Member must provide details on certificate hierarchy as well as online/offline status. Specifically, Member must describe if ICA certificates are issued out of root certificates, or out of revocable, online intermediate certificates authorities.

(k) Member is encouraged to provide any other information it deems appropriate to further explain security controls in place.

Requirements for Upper level CA or Root CA certificates

RCA1

When submitting an upper level or Root CA certificate for inclusion in the AATL, the Member must ensure:

(a) either that all end-entity certificates, all ICA(s) and all intermediate CAs part of the hierarchy under the submitted CA fulfil respectively all EE and ICA requirements; or,

(b) If only some of the subordinate (I)CAs are compliant with the ICA requirements:

1) the Member must submit compliant ICAs instead of the upper-level or Root CA; or,

2) the Member must be able to differentiate those ICA certificates through the submission to Adobe of specific certificate policy OID values. Only the certificates marked by these certificate policy OID values will be deemed as valid by Adobe Acrobat and Acrobat Reader software.

RCA2

The Member warrants that all information and representations made by the ICAs that chain up to the submitted certificate are true.

RCA3

The submitted certificate must be a X.509 V.3 certificate, profiled as per RFC 5280.

RCA4

The submitted certificate Subject Name must contain an 'organizationName' attribute (as specified in Recommendation ITU-T X.520) having as value the full registered name of the Member (as notified to Adobe) and, where applicable, an 'organizationIdentifier' attribute (as specified in Recommendation ITU-T X.520) having as value the registration number of the Member as stated in the official records.

RCA5

The Member must be generating and protecting key pair(s) for the supplied Certificate(s) in a medium that prohibits exportation and duplication that could allow unauthorized use of the private or secret keys.

A hardware security module that meet FIPS 140-2 Level 3 or equivalent provides a suitable medium.

RCA6

The Member must demonstrate robust capability to revoke the (I)CAs certificates for any (I)CAs that inherit trust from an upper level or root CA by virtue of the AATL, immediately upon any actual or suspected compromise. The Member must be willing to provide documentation to Adobe on the underlying processes and procedures. OCSP or CRL must be supported and the concerned (I)CA certificates must include the related information to enquire about the revocation status of the certificate (AIA or CDP extensions).

RCA7

The Member RCA must demonstrate capability to have its own certificate revoked in case of security compromise or, for self-signed certificates, to notify Adobe of such comprise immediately. When implementing revocation facilities, the information to enquire about the revocation status of the RCA certificate (AIA or CDP extensions) must be present in the RCA's certificate, otherwise, the Member must agree with Adobe on an incident management plan so that Adobe can swiftly remove the compromised certificate form the AATL.

RCA8

The RCA must have key length and algorithm susceptible to remain valid for the lifetime of the certificate, as recommended by authoritative researchers in the field of cryptography.

> *Note: Authoritative researchers includes NIST, ETSI, IETF, BSI, ANSSI, IAD-NSA, national authorities, academic institutions, research centers and others. For example, the ETSI TS 119 312 specification and other PKI industry studies provide guidance for the selection of key lengths and signature algorithms susceptible to remain valid for a certain amount of time.*

For RSA signature technology, a key length of 2048-bit or higher is required for RCA certificates. A key length of 3072-bit or higher is required for RCA certificates that are issued on or after 1 July 2017.

For Elliptic Curve signature technology, a key length of 256-bit or higher is required for RCA certificates. A key length of 384-bit or higher is required for RCA certificates that are issued on or after 1 July 2017.

The use of SHA256 hash algorithm or stronger is required for RCA certificates. The use of SHA1 hash algorithm is only allowed for RCA certificates that have been issued before 1 July 2013 if the Member provides publicly available means to validate that the certified public key and Distinguished Name of the certificate are genuine.

RCA9

Certificate Authority Security Controls. Members must meet all the sub-parts below:

(a) Member must provide evidence of appropriate network security controls, including IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) systems, as well as evidence of the segmentation of its key certificate issuance systems from non-related servers and systems such as marketing websites, etc.

(b) Member must have in place an incident response plan to respond to compromise or breach of its online systems as well as its certificate issuance systems.

(c) Member must demonstrate it has controls in place to prevent unauthorized or illegitimate software from executing within its systems, including but not limited to anti-virus and anti-malware software.

(d) Member must provide evidence that system administrators in Member's network do not have access to certificate issuance systems due to proper segmentation of duties and least privilege principles.

(e) Member must provide evidence of security controls in place for all accounts with certificate issuance rights.

(f) Member must provide evidence of the adoption of not only vulnerability assessment testing, including but not limited to penetration testing and application scanning (in both a credentialed and un-credentialed state), but also corrective action based on any negative results. Member should not have any common security vulnerabilities (see Common Weakness Enumeration (CWE) and Open Web Application Security Project (OWASP)) on public facing or RA / partner web sites.

(g) Member must demonstrate robust logging procedures, including aggregation of logs at alternate sites, tamper-evidence controls, and monitoring schedules.

(h) Member must provide evidences on good practices and details on its internal auditing / log monitoring practices in regards to certificate issuance (e.g. how often is Member checking certificate inventory against expected inventory?), particularly when it comes to signing certificates.

(i) Member must provide evidences on good practices and details on certificate issuance processes, to include RA and user authentication practices (as distinct from ICA5 above for subscriber/subject identification).

(j) Member must provide details on certificate hierarchy as well as online/offline status. Specifically, Member must describe if the submitted certificates are issued out of the root certificates, or out of revocable, online intermediate certificates authorities.

(k) Member is encouraged to provide any other information it deems appropriate to further explain security controls in place.