



Adobe Approved Trust List - Technical Requirements

- 1) The Applicant must own and/or operate a Certification Authority (CA).
- 2) The Applicant must use and be capable of providing x.509 v3 certificates.
- 3) The Applicant's Supplied Certificate Subject Name must contain a meaningful name of the CA (ex. cannot be "Root" or "CA1").
- 4) Non-governmental Applicants must have successfully passed within the past 18 months, and continue to pass on an annual basis, any or all of the following:
 - a) WebTrust for CA audit;
 - b) ETSI 101 456 v1.4.3 audit;
 - c) ETSI 102 042 v1.2.4 audit;
 - d) ISO 21188:2006; and/or
 - e) German Digital Signature law audit
- 5) Government Applicants may either provide audit documents as in (5) above or must provide documentation / statements as to audit equivalency.
- 6) The Applicant must be generating and storing key pair(s) for the Supplied Certificate(s) in a medium that prevents exportation or duplication such as hardware security modules that meet FIPS 140-2 Level 3 or equivalent.
- 7) The Applicant must demonstrate the use of strong identification and authorization procedures and be willing to provide documentation to Adobe on these processes. In particular, the Applicant must:
 - a) ensure that Subscribers and ICAs generate public key pairs using a trustworthy system, or generated in a secure hardware token and take all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key; and
 - b) warrant that all information and representations made by the Subscriber and ICAs that chain up to the Supplied Certificate are true;
- 8) Applicant CA must demonstrate 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 the identity of the subscriber is no longer associated with the approving entity.

9) Supplied Certificate key sizes should be at least RSA 2048-bit. Hash algorithm should be at least equivalent to SHA-1 or the SHA-2 family (256/384/512).

10) Applicant whose CA is certified

- a) as Qualified by an EU member state per the EU Signature Directive (Directive 1999/93/EC) which may be validated by means of the Supervisory Authorities within the member state, or is certified
- b) as meeting the Medium Hardware Assurance Requirements of: the US Federal Bridge (http://www.cio.gov/fpkia/documents/crosscert_method_criteria.pdf), the SAFE-BioPharma bridge, or the CertiPath commercial bridge by privilege of having the Supplied Certificate cross-certified to the bridge,

shall be considered as compliant with items 2-9 above, provided that such claim may be validated, and provided that Adobe reserves the right to request additional proof and documentation.

11) All intermediate and end entity certificates under the Applicant's Supplied Certificate must be compliant with items 6-9 above, with the exceptions that requirements for end-entity certificates are reduced to:

- a) Key length of 1024-bit
- b) Hardware certified to FIPS 140-2 Level 2; Common Criteria, ISO 15408, Protection Profile: CWA 14169; or Certification as a Secure Signature Creation Device (SSCD) from an EU government entity.

If only *some* of the certificates are compliant with these items, then the Applicant **must** be able to differentiate those certificates through either the submission to Adobe of specific intermediate CAs (ICAs) or Policy OID values.

12) The Applicant must provide to Adobe its Supplied Certificate in advance in order to check compatibility with the Trust List prior to official insertion on the List.

13) The Applicant must agree to annual validation of its ability to meet the Technical Requirements, which can include submission to Adobe of annual audit results.

14) The Applicant must be able to meet the Technical Requirements throughout the term of the Member Agreement.

15) Certificate validation via OCSP is not required for end entity certificates, but is highly recommended. In any case, validation status via CRL must be available.

16) RFC 3161 timestamps are not required for end entity certificates, but are highly recommended.

- 17) The Applicant is not required to add custom OIDs to their certificates as part of the AATL. However, Applicant should consider adding appropriate Adobe-specific OIDs to new certificates to allow for automatic time stamping (RFC3161) and OCSP revocation checking within Adobe products for long term validation purposes.