Adobe Approved Trust List Technical Requirements Version 1.4

Technical Requirements

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 Reader® software. Essentially, both Acrobat and Reader have been programmed to reach out to a web page to periodically download a list of trusted "root" digital certificates. Any digital signature created with a credential that can trace a relationship ("chain") back to the high-assurance, trustworthy certificates on this list is trusted by Acrobat and Reader.

Requirements

1. The Member must own and/or operate a Certification Authority (CA).
2. The Member must use and be capable of providing x.509 v3 certificates.
3. The Member's Supplied Certificate Subject Name must contain a meaningful name of the CA (ex. cannot be "Root" or "CA1").
4. Non-governmental Members must have successfully passed within the past 18 months, and continue to pass on an annual basis, any or all of the following:
   - 4.1. WebTrust for CA audit;
   - 4.2. ETSI 101 456 audit;
   - 4.3. ETSI 102 042 audit;
   - 4.4. ISO 21188:2006; and/or
   - 4.5. German Digital Signature law audit
5. Government Members may either provide audit documents as in (5) above or must provide documentation / statements as to audit equivalency.
6. The Member 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 Member must demonstrate the use of strong identification and authorization procedures and be willing to provide documentation to Adobe on these processes. In particular, the Member must:
   - 7.1. 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
   - 7.2. warrant that all information and representations made by the Subscriber and ICAs that chain up to the Supplied Certificate are true;
8. Member 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 or ECC P256. Hash algorithm should be at least equivalent to SHA-1 or the SHA-2 family (256/384/512) up to July 1, 2013, then SHA-2 only.
10. Member whose CA is certified
    - 10.1. 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
    - 10.2. 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 generally 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 Member's Supplied Certificate must be compliant with items 6-9 above, with the exceptions that requirements for end-entity certificates are reduced to:
    11.1. Key length of 1024-bit up to July 1, 2013, then 2048-bit key lengths or ECC P256 must be issued
    11.2. 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 Member must be able to differentiate those certificates through either the submission to Adobe of specific intermediate CAs (ICAs) or Policy OID values.

12. Certificate Authority Security Controls. Members must meet all of the sub-parts below, or provide evidence as to compensating controls, as determined by Adobe at its sole discretion. Adobe will agree to keep this information confidential per the terms of the AATL Member Agreement.
    12.1. Member must provide evidence of appropriate network security controls, including IDS/IPS 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.
    12.2. 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.
    12.3. 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.
    12.4. 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.
    12.5. Member must provide evidence of security controls in place for all accounts with certificate issuance rights.
    12.6. Member must provide evidence 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 CWE / OWASP) on public facing or RA / partner sites.
    12.7. Member must provide 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.
    12.8. Member must demonstrate robust logging procedures, including aggregation of logs at alternate sites, tamper-evidence controls, and monitoring schedules.
    12.9. Member must provide details on certificate issuance processes, to include RA and user authentication practices (as distinct from Requirement 7 above for Subscriber identification required above).
    12.10. Member is encouraged to provide any other information it deems appropriate to further explain security controls in place.
    12.11. Member must provide details of certificate hierarchy as well as online/offline status. Specifically, Member must describe if certificates are issued out of the root certificates, or off of revocable, online intermediate certificates authorities.
13. Member must agree to notify Adobe immediately (unless otherwise restricted by law enforcement or government authorities) of any compromise, breach, certificate mis-issuance, or suspicion thereof, on any server, PC or other system or endpoint that is logically connected to certificate issuance and management systems. Notice can be sent via email to AATLNotification@adobe.com or other email address provided by Adobe.
    13.1. Member must provide Adobe with details of the breach and a remediation / action plan within 3 days of the notification.
14. The Member must provide to Adobe its Supplied Certificate and sample signed PDF documents in advance in order to check compatibility with the Trust List prior to official insertion on the List.

15. The Member must agree to annual validation of its ability to meet the Technical Requirements, which can include submission to Adobe of annual audit results.
16. The Member must be able to meet the Technical Requirements throughout the term of the Member Agreement.
17. 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.
18. RFC 3161 timestamps are not required for end entity certificates, but are highly recommended.
19. The Member is not required to add custom OIDs to their certificates as part of the AATL. However, Member 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.
20. The Member must enforce a traditional public key infrastructure model, wherein the signer is in physical possession and control of a hardware security token or module that contains the private key. Newer models wherein a signer remotely accesses the private key on a server are possible, if the private key resides on an HSM and strong authentication methods are used, but will still need to be approved by Adobe.