Post Jan 2016 SHA-1 Issuance Request Procedure

Version 1.0 - June 3rd 2016

The SHA-1 hash algorithm, which first showed signs of weakness in 2005, is now considered dangerously susceptible to collision attacks[1]. Any use of a publicly trusted CA private key to sign a SHA-1 hash exposes the Internet to significant risk. Accordingly the CA/B Forum's Baseline Requirements prohibit the issuance of new certificates with a SHA-1 based signature algorithm after 1st January 2016[2]. Unfortunately some users of the publicly trusted PKI have failed to migrate in time and are still reliant on SHA-1 certificates for exceptionally critical functionality[3]. These procedures outline the steps a CA can take to request an exception and obtain a new SHA-1 Certificate.

Note that nothing in this procedure guarantees any such exceptions will be granted. It details the information that should be provided in the request and outlines mitigations, such as counter-cryptanalysis, that might lower the risk of issuing a particular SHA-1 certificate.

Step One: Request

The Subscriber's CA should send an email addressing each of the following points to public@cabforum.org, CCing a representative of the Subscriber.

1. The name and contact details of the Subscriber.
2. A description of the infrastructure that requires SHA-1 Certificates for correct operation.
3. A detailed description of what steps have already been taken remediate the situation without needing a new SHA-1 Certificate (such as issuing from a pulled root), and why have they failed.
4. When would new SHA-1 Certificates need to be issued to ensure continuity?
5. A detailed description of the impact if new SHA-1 Certificates are not obtained before that date.
6. What is the anticipated date the transition from SHA-1 Certificates will be complete?
7. When and how did the Subscriber first became aware of the SHA-1 sunset?
8. What procedures are in place to ensure a similar exception will not be required when standards currently in use are deprecated?
9. The number of Requested Certificates.
10. For each Requested Certificate:
    a. The proposed tbsCertificate in DER format, i.e. the exact bit pattern that would be signed. (Note this could be attached separately and a SHA-256 hash of the DER

[1] https://sites.google.com/site/itstheshappening/
[2] See §7.1.3 of the Baseline Requirements
[3] https://blog.mozilla.org/security/2016/02/24/payment-processors-still-using-weak-crypto/

file included in the signed request). The notBefore date may be up to 14 days in the future to accommodate the review time.

b. A corresponding human readable version, for reference.
c. A crt.sh link to the Existing Certificate.
d. Additional information as required by Existing Certificate Information section.

Existing Certificate Information

Ideally the proposed tbsCertificate should correspond to an Existing Certificate logged in at least two Certificate Transparency log trusted by one or more Application Software Suppliers, with an audit proof to a Signed Tree Head with a timestamp prior to 1st January 2016 and differing only by:

- signature AlgorithmIdentifier
- Serial Number, which must have at least 60 bits of entropy
- Validity, which must have a notAfter on or before 31st December 2016

If the Existing Certificate was not logged prior to 1st January 2016, any evidence that might help establish when the Existing Certificate's key pair was created should be provided if available.

If other fields than those listed above need to change (for example if a new issuer is needed because the original subordinate CA is no longer operating) then each discrepancy should be explained and crt.sh links provided to certificates which show the values are expected. Failing that, other evidence that the mismatching values have expected values such as links to CP/CPSs should be provided.

If a new key pair must be used for the new SHA-1 Certificate being requested, details of how and by whom the new key was generated must be supplied along with an explanation of why a new key was needed.

The number, type, and details of the differences between the Existing Certificate and the Requested Certificate will be taken into account by the Application Software Suppliers when considering the request.

Notes

The request must be S/MIME or PGP signed in a way that Application Software Suppliers can validate the authenticity of the request.

The number and frequency of requests is intended to be low. Application Software Suppliers have no obligation to consider requests for any reason including if they are frequent and/or contain an excessive number of Requested Certificates.

Step Two: Consultation

After the request has been made, a period of consultation of at least 10 business days to allow interested parties to:

- Verify the authenticity of the request.
- Request and receive clarification of information provided in the request if needed.
- Independently confirm any verifiable details provided in the request, such as certificate inclusion in CT logs.
- Perform counter-cryptanalysis, such as using tools provided by Dr. Marc Stevens[4]
- Weigh the risk to ecosystem and user security against the benefit of preventing breakage.

Application Software Suppliers are encouraged to give weight to signed and verifiable attestations by cryptographic experts that tbsCertificates are free from collisions to an 80 bit security level. CAs are encouraged to ensure such analysis takes place.

Step Three: Response

At some point after 10 business days have elapsed, Application Software Suppliers may, independently and entirely at their own discretion:

- Refuse the exception.
- Fail to answer, which is an implicit refusal.
- Refuse the exception with recommendations to amend the request and re-apply (though they are encouraged to provide such feedback during the consultation window).
- Grant the exception for a subset of Requested Certificates.
- Grant the exception for all Requested Certificates.

The response must be S/MIME or PGP signed in a way that the requesting CA can validate the authenticity of the request.

Step Four: Issuance

If the CA wishes to continue with issuance, for each certificate:

- The CA must perform at least OV level vetting
- The Exceptionally Issued Certificate must be submitted to and accepted by at least two Certificate Transparency log trusted by one or more Application Software Suppliers.
- The CA must reply to public@cabforum.org with details of the issuance including:

[4] https://marc-stevens.nl/research/

- The Exceptionally Issued Certificate in PEM format.
- A crt.sh link to the Exceptionally Issued Certificate.
- A crt.sh link to a valid BR compliant SHA-2 certificate with corresponding Subject Alternate Name.

Note that even with a granted exception, the issuance will still be contrary to CA/B Forum Baseline Requirements and as such CAs can expect to receive a qualified or otherwise annotated audit due to the issuance.

Any Application Software Supplier who did not grant an exception may treat the issuance as they would any other mis-issuance and take whatever action they feel appropriate.

Step Five: Post Issuance

Once the CA has confirmed the issuance, interested parties are encouraged to:

- Verify that the tbsCertificate of the Exceptionally Issued Certificate exactly matches that in the request
- The Exceptionally Issued Certificate has valid audit proofs in the CT logs

Each Application Software Supplier that granted an exception should also perform the same verification and if successful, make a note of the exception. When reviewing the CA's audit for the period covering the issuance(s), the Application Software Supplier will discount the qualifications that correspond exactly to the granted exception.

Definitions:

Certificate Transparency log: A certificate log as described in RFC 6962.

crt.sh link: A URL in the form https://crt.sh/?q=<hex_encode_ sha256_cert_hash> which uniquely specifies a certificate and facilitates issuing audit proof queries against Certificate Transparency logs.

Exceptionally Issued Certificate: A SHA-1 Certificate issued by a publicly trusted CA after 1st January 2016.

Existing Certificate: A SHA-1 Certificate that was issued in accordance with the CA/B Forum Baseline Requirements in effect at the time of issuance, for which the Requested Certificate could be considered a renewal.

Requested Certificate: The tbsCertificate that when signed by a CA key becomes an Exceptionally Issued Certificate.

SHA-1 Certificate: An X.509 certificate with a signatureAlgorithm that uses SHA-1 and that chains, directly or indirectly, to an anchor trusted by one or more Application Software Suppliers.

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

tbsCertificate: The data structure defined in RFC 5280[5]

[5] https://tools.ietf.org/html/rfc5280#section-4.1