DRAFT Ballot 15X - Legacy Verified (LV) Certificates

Preamble

The current CA/B Forum Baseline Requirements – v1.3.1 published on September 28, 2015 – prohibit issuance of SHA-1 certificates as of January 1, 2016. This change was added as a result of ballot #118 passing on October 16, 2014. At that time, the stated purpose was that “several Application Software Providers” have announced deprecation of SHA-1 in their software (due to perceived risk of collisions).

Since then, independent tests conducted by Facebook and CloudFlare have concluded that, at minimum, anywhere from 2-7% of global user agents are unable to use HTTPS sites utilizing SHA-2 signature algorithms [1] [2]. In certain disadvantaged, war-torn areas of the world, such figures are considerably higher. While existing and well-established enterprises can stockpile certificates, these areas represent some of the greatest growth opportunities and potential for internet access to change people’s lives in the near future. Globally, many thousands of new zones are added each day that require provision of new certificates. Being unable to obtain certificates to reach local audiences during the SHA-1 phase-out period would present a significant obstacle to better serving these populations with new opportunities and services.

Though we believe strongly that modern browsers should continue to remove support for SHA-1 certificates, we do not believe that the tens of millions of users unable to utilize SHA-2 should be locked out when there is a responsible manner in which they can continue to be served. We also are in support of full (certificate) transparency for these LV certificates, and would like to see all Certificate Authorities log their issuance to a publicly accessible location.

This ballot proposes a responsible way to serve these SHA-1 certificates to user agents that cannot, for legacy/technical reasons, validate SHA-2 certificates. It also specifies measures to significantly minimize the risk that a collision could be maliciously crafted by an attacker. Since the current research points to the possibility of birthday-paradox collisions being generated, and not full pre-image attacks, we believe that the 20-bit entropy requirement is sufficient to prevent the kinds of attacks seen against CAs during the MD5 transition.

[1] - https://blog.cloudflare.com/sha-1-deprecation-no-browser-left-behind/
[2] - https://www.facebook.com/notes/alex-stamos/the-sha-1-sunset/10153782990367929

Motion Begins

Amend the Baseline Requirements v1.3.1 as follows:

1. Amend Section 1.2.2 (Relevant Dates), Compliance Date 2016-01-01:

2016-01-01	7.1.3	CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm **except to Applicants requesting Legacy Validated Certificates (as defined elsewhere in this document). Such Certificates MUST NOT have Expiry Dates greater than 31 March 2019.**
201**9-03-31**	7.1.3	CAs MUST NOT issue OCSP responder certificates using SHA-1 (inferred).

2. Amend Section 7.1 (Certificate Profile):

The CA SHALL meet the technical requirements set forth in Section 2.2, Section 6.1.5, and Section 6.1.6.

If the Certificate asserts the Policy Identifier of 2.23.140.1.2.99, then the CA MUST generate non-sequential Certificate serial numbers that exhibit at least 20 bits of entropy.

Certificates asserting Policy Identifiers other than 2.23.140.1.2.99 SHOULD generate non-sequential Certificate serial numbers that exhibit at least 20 bits of entropy.

3. Amend Section 7.1.3 (Algorithm object identifiers) to:

Effective 1 January 2016, CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm **other than to Applicants adhering to all of the Legacy Validated ("LV") requirements put forth in this document.** CAs MAY continue to sign certificates to verify OCSP responses using SHA1 until **31 March 2019**. This Section 7.1.3 does not apply to Root CA or CA cross certificates. CAs MAY continue to use their existing SHA-1 Root Certificates. SHA-2 Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate.

Effective 16 January 2015, CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017 because Application Software Providers are in the process of deprecating and/or removing the SHA-1 algorithm from their software, and they have communicated that CAs and Subscribers using such certificates do so at their own risk. **Effective [XX] December 2015, CAs MUST NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with Expiry Dates greater than 31 March 2019.**

4. Amend Section 7.1.6.1 (Reserved Certificate Policy Identifiers):

This section describes the content requirements for the Root CA, Subordinate CA, and Subscriber Certificates, as they relate to the identification of Certificate Policy.

The following Certificate Policy identifiers are reserved for use by CAs as an optional means of asserting compliance with these Requirements as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1), if the Certificate complies with these Requirements but lacks Subject Identity Information that is verified in accordance with Section 3.2.2.1.

If the Certificate asserts the policy identifier of 2.23.140.1.2.1, then it MUST NOT include organizationName, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) subject-identity-validated(2)} (2.23.140.1.2.2), if the Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with Section 3.2.2.1.

If the Certificate asserts the policy identifier of 2.23.140.1.2.2, then it MUST also include organizationName, localityName, stateOrProvinceName (if applicable), and countryName in the Subject field.

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) legacy-validated(99)} (2.23.140.1.2.99), if the Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with Section 3.2.2.1.

If the Certificate asserts the policy identifier of 2.23.140.1.2.2, then it MUST also include organizationName, localityName, stateOrProvinceName (if applicable), and countryName in the Subject field.

5. Amend Section 7.1.6.4 (Subscriber Certificates) to:

A Certificate issued to a Subscriber MUST contain one or more policy identifier(s), defined by the Issuing CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Requirements. CAs complying with these Requirements MAY also assert one of the reserved policy OIDs in such Certificates.

If the Certificate is to use the SHA-1 signature algorithm, it MUST (a) assert the policy identifier of 2.23.140.1.2.99 and (b) be issued under a Subordinate CA that was created exclusively for the purpose of issuing such Legacy Validated Certificates.

The issuing CA SHALL document in its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

6. Amend Section 9.6.3 (Subscriber representations and warranties) to:

The CA SHALL require, as part of the Subscriber or Terms of Use Agreement, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's agreement to the Terms of Use agreement.

The CA SHALL implement a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement.

The Subscriber or Terms of Use Agreement MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate**: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;

5. **Reporting and Revocation**: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;
6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance**: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.
9. **Use of LV Certificates**: **An obligation and warranty to serve Legacy Validated Certificates only (a) after the Subscriber has first obtained a SHA-2 signed certificate (i) covering the same *extensions:subjectAltName* and (ii) with organizationName, localityName, stateOrProvinceName (if applicable), and countryName in the Subject field and (b) to Relying Parties whom the Subscriber reasonably believes may not be able to utilize Certificates signed using more modern digests, such as SHA-2;**
10. **Termination of Use of LV Certificates: An obligation and warranty to promptly cease all use of Legacy Validated Certificates when the CA/Browser Forum is notified that a reproducible method for forcing applications from major Application Software Suppliers is discovered that (a) causes said applications to accept and validate LV Certificates that the applications should otherwise have rejected due to their explicit SHA-1 rejection logic and (b) cannot be resolved by technical changes made either by the Application Software Suppliers or the Subscriber;**

Motion Ends