Migration to SHA-2 Certificate Authority

Q: Migration to SHA-2 Certificate Authority

- Why is MIT migrating to a new certificate authority?
- What is the difference between SHA-1 and SHA-2 certificates?
- How will I be affected by the change of certificate authority?

Context

- Applies to all operating systems and platforms

Answer

- MIT is transitioning to the use of SHA-2 for certificates. In the near future, multiple web browsers such as Firefox, Internet Explorer, and Chrome, among others, will stop accepting the old SHA-1 certificate hash which has been used in the past. To prevent these browsers from refusing to accept MIT server certificates, MIT has decided to migrate to the SHA-2 hash for protection of our certificates.
- According to Google, Chrome will begin treating SHA-1 based certificates valid past January 1 2017 as untrustworthy starting with the release of Chrome 39 in November 2014. Other browsers are also making plans to deprecate the use of SHA-1 in certificates.
- Users of certificates should make plans to upgrade certificates before software begins rejecting the old certificate hash.
- New MIT certificates will be signed by the "InCommon RSA Server CA" and will use 2048-bit RSA encryption as well as a SHA-256 hash.

Additional Browser Information

Firefox

Firefox will introduce a warning for certificates valid past January 1, 2017 using SHA-1, and will reject such certificates entirely as of January 1, 2017: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Chrome

In releases 39 through 41, Google will gradually phase out support for SHA-1 certificates entirely:
http://googleonlinesecurity.blogspot.com/2014/09/gradually-sunsetting-sha-1.html

Internet Explorer

Internet Explorer will stop accepting SHA-1 based end-entity certificates by January 1, 2017:
http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx