Deprecation of SHA-1 Hashing Algorithm in 2017

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT, all versions

DISCUSSION

According to a Google blog post1:

The SHA-1 cryptographic hash algorithm has been known to be considerably weaker than it was designed to be since at least 2005 — 9 years ago. Collision attacks against SHA-1 are too affordable for us to consider it safe for the public web PKI. We can only expect that attacks will get cheaper.

SHA-1's use on the Internet has been deprecated since 2011, when the CA/Browser Forum, an industry group of leading web browsers and certificate authorities (CAs) working together to establish basic security requirements for SSL certificates, published their Baseline Requirements for SSL. These Requirements recommended that all CAs transition away from SHA-1 as soon as possible, and followed similar events in other industries and sectors, such as NIST deprecating SHA-1 for government use in 2010.

Support for SHA1 based SSL certificates will be dropped by Microsoft/Windows in 2017.

- Windows will no longer trust certificates signed with SHA-1 after 2/14/2017

"Server-Authentication Certificates: In summer 2016, Internet Explorer and Edge stopped showing the lock icon on web pages secured with SHA-1 certificates. Effective February 14, 2017, Windows will no longer trust certificates signed with SHA-1."2

References:

- https://security.googleblog.com/2014/09/gradually-sunsetting-sha-1.html

You can find more information at the following web pages:

- https://www.digicert.com/sha-2-ssl-certificates.htm
- https://blogs.windows.com/msedgedev/2016/04/29/sha1-deprecation-roadmap/#0Q7536jFwkEcLGo5

Deprecation of SHA-1 Hashing Algorithm in 2017

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11325/Deprecation-of-SHA1-Hashing-...