

Transitioning to SHA-2 for SSL

SHA-2 is a family of cryptographic hashing algorithms developed by NIST (National Institute of Standards and Technology) in order to replace the aging SHA-1 hashing algorithm which may have mathematical weaknesses. The SHA-1 cryptographic hash algorithm has been known to be considerably weaker than it was designed to be at 2005. As of now SHA-2 hashing algorithms (SHA-256, SHA-384, SHA-512) are already widely supported.













Google accelerated the timeline for browser checking of SHA-1 in web server SSL certificates so that Chrome will display security notices where SHA-1 is encountered. Google plans to deprecate SHA-1 on upcoming releases of Chrome starting with version 39.

Even though the CA/Browser Forum (an international committee of leading CA's and Browsers working to define sectorial best practices) is also specifying migration to SHA-2 in their Baseline Requirements, Google, Microsoft and Mozilla are driving the industry to the January 2017 date when they will stop trusting all SHA-1 Certificates issued under public roots.

Important date for the end of support for SHA-1:

January 1, 2017 Microsoft will cease trusting SSL Certificates using SHA-1,
Mozilla will cease trusting SSL Certificates using SHA-1,
Google will cease trusting SSL Certificates using SHA-1,

Google plans on placing visual marks within the browser; all based on the version of the browser, date of use and certificate's expiration date which is shown below;

| Chrome Version | Expiration Dates | | | |
|-----------------------------------|---|---|---|---|
| | SHA-1 (31.12.2015) | SHA-1 (31.5.2016) | SHA-1 (31.12.2016) | SHA-1 (after 1.1.2017) |
| Chrome 39 (Expected Nov. 2014) |  |  |  |  |
| Chrome 40 (Expected Dec. 2014) |  |  |  |  |
| Chrome 41 (Q1 2015) |  |  |  |  |

Note: Most applications, servers and browsers already support certificates created by SHA-2, however some older operating systems such as Windows XP prior to Service Pack 3 and some mobile devices do not.

TURKTRUST, as a certification authority, will support deprecation of SHA-1 and transition to SHA-2 for SSL certificates. We will be working with each of our customers to ensure a seamless transition.