SHA1 Certificates

In 2013, Microsoft announced that it would deprecate SHA-1 certificates in January 2017, and as a result certificate authorities, including QuoVadis, began implementing a program to move customers from SHA-1 certificates to SHA-256 certificates by the end of 2016.

However, this timeline was recently greatly accelerated with an announcement from Google that it would stop supporting SHA-1 certificates a year earlier – January 1, 2016. This move is intended to force certificate users to start moving to SHA-256 certificates as soon as possible. Microsoft & Mozilla (IE & Firefox) have announced they are likely to follow similar timelines, although no official details have yet been provided.

Google has announced the following timeline (Chromium release calendar is available at http://www.chromium.org/developers/calendar):

- Chrome release 39, September 26, 2014 All SHA-1 certificates expiring after December 31, 2016 will display degraded HTTPS feedback in the address bar.
- Chrome release 40, November 7, 2014 All SHA-1 certificates expiring after June 1, 2016 will display degraded HTTPS feedback in the address bar. Affects 2-year certificates issued on or after June 1, 2014.
- Chrome release 41, January 12, 2015 All SHA-1 certificates expiring after December 31, 2015 will display degraded HTTPS feedback in the address bar.

In response to this recent change, AusCERT/QuoVadis has accelerated its SHA-256 Deprecation plans.

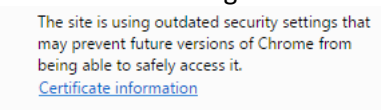
How this affects you

Although not finalized by Google, the following images indicate the expected address bar treatment.

The site uses SSL and is secure but Google Chrome has detected minor issues.

The site uses SSL, but Google Chrome has detected either high-risk insecure content on the page or problems with the site's certificate.

This is what is being shown currently in Chrome:



It may be that by the end of 2015, Chrome will not let users navigate to SHA1 protected sites at all.

What you should do

You should replace all of your affected SHA-1 certificates as soon as possible, (especially all certificates that expire after the end of 2015).

You should also plan a transition strategy of all your certificates to SHA-256 as soon as possible to avoid downtime – if you encounter network/user issues AusCERT/QuoVadis will work with you to identify and resolve them.

A list of servers and applications that are compatible with SHA-256 is available at the following link https://casecurity.org/wp-content/uploads/2014/09/SHA-256-Support-List.pdf.

Please contact au.support@quovadisglobal.com if you have any questions.

QuoVadis Online Security Ltd
Tel +44 (0) 333 666 2000
http://www.quovadisglobal.co.uk