CSC® DIGITAL BRAND SERVICES
CORPORATION SERVICE COMPANY®

Digital Certificate Industry Changes

The continuing need to strengthen security techniques has brought about the need for digital certificates with SHA-2 hashing algorithms. In 2011, the CA/B Forum recommended that all certificate authorities move away from the SHA-1 algorithm.

Microsoft, Google and Mozilla have now announced timelines for when their internet browsers will no longer recognize certificates using the SHA-1 algorithm as “trusted”. This means after specified dates, websites secured by digital certificates with a SHA-1 signature as part of the chain will display warning messages if viewed in Internet Explorer, Chrome, Firefox and potentially other browsers. The announcements from Microsoft, Google and Mozilla have prompted the Certificate Authorities to implement these changes based on the timeframes announced.

It is important to note that not all servers support SHA-2 algorithms. Customers should check their server documentation or with their IT department to confirm SHA-2 is supported.

WHAT ACTION DO YOU NEED TO TAKE?

As best practice, all new certificates should be requested with SHA-2 hashing. It is important to note that not all servers support SHA-2 algorithms. You should check your server documentation or with your IT department to confirm whether SHA-2 is supported.

As of September 22, 2014, CSC will issue certificates with SHA-2 hashing as default, regardless of what is coded in the CSR. If you require a SHA-1 certificate, please request this through your Client Service Partner. SHA-1 certificates will be available for purchase until December 31, 2014.

Existing certificates with SHA-1 hashing that expire on or after Jan 1, 2015 should be reissued with SHA-2 hashing. Your Client Service Provider will be in contact with you soon about any certificates that are affected by these changes.

IS THERE A FEE TO REISSUE WITH SHA-2?

No, CSC does not charge a fee for reissue of certificates.

WHEN IS THIS HAPPENING?

The dates outlined below are a timetable dictated by the respective browsers and are subject to change based on the Certificate Authorities' own timelines.

QUICK REFERENCE TABLE

Effective Date	Certificate Expiration Date	Message
Sep 2014	Jan 1, 2017 or later	Chrome warning: "secure, but with minor errors"; displays lock with yellow triangle.
	Any	CSC will issue SHA-2 certificates by default
Q3-4 2014	Jan 1, 2017 or later	Mozilla (Firefox) will start rejecting SHA-1 SSL certificates.
Nov 2014	June 1, 2016-December 31, 2016	Chrome warning: "secure, but with minor errors"; displays lock with yellow triangle.
	Jan 1, 2017 or later	Chrome warning: "neutral, lacking security", and will display a blank page (no lock).
Q1 2015	June 1, 2016-December 31, 2016	Chrome warning: "secure, but with minor errors"; displays lock with yellow triangle.
	Jan 1, 2017 or later	Chrome warning: "affirmatively insecure"; displays a lock with a red X
Jan 2016	Any	Microsoft will cease to trust code signing certificates with SHA-1
Jan 2017	Any	Microsoft will cease to trust digital certificates with SHA-1

WHAT HAPPENS IF I DON'T TAKE ACTION?

If you do not replace SHA-1 certificates before the dates above, your sites hosting these certificates will no longer be trusted by Microsoft software like Internet Explorer and Windows, Google Chrome and Mozilla Firefox. Other vendors are likely to follow suit, which means your certificate won't be trusted by other browsers like Safari as well.