Tech Alert

from the Customer Delivery Division

"Your Gateway to OTech Services"

TA 14-22: Secure Certificate Service SHA-1 Deprecation

ATTENTION: Secure Certificate Service Customers

ACTION REQUESTED: Verify SHA-2 compatibility of secured systems

DUE DATE: Prior to certificate expiration

Overview:

The use of the certificate signing algorithm SHA-1 has been deprecated in favor of the newer and more secure SHA-2 algorithm. OTech will replace existing SHA-1 certificates issued through the OTech Secure Certificate Service with SHA-2 at no charge.

Policy Change:

As of September 8, 2014, the Office of Technology Services (OTech) began issuing SHA-2 certificates by default. This change was due to the recent SHA-1 deprecation announcement, and browser and operating system change announcements made by Google and Microsoft. Please read the announcement from our Certificate Authority for additional details.

Next Steps:

Next steps vary by department based on the type of system utilizing the certificate. OTech recommends that customers read the linked announcement above to determine the appropriate course of action for their affected systems. This document includes the timelines for the changes, and customers will have to determine their individual "due date" based on the impact of these changes.

Customers with non-public facing, non-Windows systems will not be impacted by the Google Chrome or Microsoft changes. However, when non-impacted customers renew their existing certificate(s), SHA-2 certificates will be issued by default. If your system is not SHA-2 compliant, you can request a SHA-1 certificate on a temporary basis.

Requested Action:

Prior to requesting a secure certificate from OTech, ensure that your system is compatible with the SHA-2 encryption algorithm. In cases of legacy incompatibility, SHA-1 certificates may be requested but they must expire before January 1, 2016. In addition, generation of SHA-1 certificates may incur additional processing time. Due dates for taking action are dependent on the actual use of the certificate. See the announcement for actual timeframes for your type of certificate.

If you would like your existing SHA-1 certificate replaced with a SHA-2 certificate prior to expiration, please submit a Work Order to the OTech Service Desk. If the certificate is customer installed, please attach your Certificate Signing Request (CSR) to the Work Order.

Due Date:

Varies by customer—prior to certificate expiration. Please see the timelines in the linked announcement above.

Contact:

If you have questions or need further clarification, please contact Secure Certificates Services at Certificate_Services@state.ca.gov or your OTech Account Lead. If you are unsure who your Account Lead is, please use the Account Lead Lookup, or call the Customer Delivery Division at (916) 431-5476.

Office of Technology Services • P.O. Box 1810 • Rancho Cordova, CA 95741-1810
Phone: 916-431-5390 • Fax: 916-463-9916 • www.otech.ca.gov • OTechTechAlert@state.ca.gov