

VerifiedByVisa

Monday, July 18, 2016 2:50 PM

Dear Customer,

CA would like to clarify certain points related to the SHA2 certificates for SaaS instances. In reference to an earlier communication, we would like to state that ACS server certificates will be upgraded to SHA2 in phases. This is largely driven by proximity to the SHA1 certificate expiry date.

CA is continuing to work with Visa and will undertake every measure needed to ensure that service availability is not interrupted.

Below are a few key milestones.

- 1. Effective 31 March 2016**, Visa stopped allowing **RC4-encrypted connections** to any Verified by Visa hardware: CA Transaction Manager does not need any change to comply with this requirement. Our software has inbuilt support for newer ciphers that Visa is using and we have not noticed any impact on transactions due to this change.
- 1. Effective 30 June 2016**, Visa has enabled the use of TLS versions 1.1 and 1.2 encryption for all Verified by Visa hardware: All instances of CA Transaction Manager are upgraded to version 7.5.3 which supports TLS1.1 and 1.2.
- 1. Effective 30 June 2018**, Visa has disabled the use of TLS version 1.0 and requires that secure connections to any Verified by Visa hardware use TLS version 1.1 encryption or higher: CA currently supports newer TLS protocols TLS1.1 and TLS 1.2 effective April 15th, 2016.
- 1. Effective 8 April 2016**, Visa began issuing SHA-2 digital signing certificates and will stop issuing SHA-1 digital certificates: CA currently requests only SHA-2 Server certificates for all instances in SaaS. These certificates will be deployed in production as and when they approach expiry and not by 8 April 2016 as stated before. We anticipate this activity to be ongoing until all server certificates are replaced. CA has and will continue to initiate certificate request for all member signing certificates in production for Visa and expects this to be a continual process. *Existing signing certs will continue to work as-Is till end of year with no impact.*
- 1. Effective 1 January 2017**, CA / Browser Forum deadline: No SHA-1 certificates will be accepted after this date: We intend to complete migration for all Visa issued certificates to SHA-2 by the end of 2016 and not by 30th June 2016 as stated earlier.

CA has a community page for customers to ask and discuss any topics related to this issue, as always feel free to contact the CA Support team at by phone at 1-866-992-7268 (or your regional support contact) or submitting a request at support.arcot.com.

For information on how to use community page, please follow this link, a copy of this communique is at this link.

We thank you for choosing CA to serve your 3DSecure needs.

Regards,
The CA Payment Security Team

Copyright © 2016 CA, Inc. All rights reserved. All marks used herein may belong to their respective companies. This document does not contain any warranties and is provided for informational purposes only.