SHA-1 Re-Issue Exception Request

Symantec will send an email addressing each of the following points to public@cabforum.org, copying a representative of the Subscriber (TSYS).

1. The name and contact details of the Subscriber.

TSYS Acquiring Solutions, LLC
8320 South Hardy Drive
Tempe, AZ 85284
Correspondence e-mail: acq-tdsnotice@tsys.com; encryptionservicesoperations@tsys.com
Primary Contact: Bryan Smoak - bryansmoak@tsys.com
Secondary Contact: Janine Hill - jhill@tsys.com

2. A description of the infrastructure that requires SHA1 Certificates for correct operation.

Apache 2.xx and Tomcat 5+

3. A detailed description of what steps have already been taken remediate the situation without needing a new SHA1 Certificate (such as issuing from a pulled root), and why have they failed.

Due to the reliance on Operating System (Windows, OSX, Linux, etc.) Certificate Stores used by many POS Applications/Integrations and POS devices (i.e. iOS, Android) using a deprecated root would result in substantial manual intervention, connection failures and ultimately a very poor consumer experience if the pulled root did not exist in the Merchants POS Application or Device. While TSYS, TSYS Clients and valued Development Partners have made substantial improvements in the impacted portfolio (from 300K to 60K) since January 2016, there is still a substantial portfolio (60K) of POS application / devices outstanding that must be remediated.

4. When would new SHA1Certificates need to be issued to ensure continuity?

31 July 2016

5. A detailed description of the impact if new SHA1 Certificates are not obtained before 31 July 2016.

Operational Challenges

- The problem is that many of the terminals are older technology and cannot be upgraded quickly, do not have remote update options for SSL/TLS (like Operating Systems) or have used an embedded SSL/TLS client that must be replaced.
- Additional issues of concern to ensure timely and expedited upgrades from SHA-1 to SHA-2 is the growing use of integrated software at the point-of-sale. These integrated systems have levels of complexity that present further challenges to ensure they are adequately and accurately enabled to move to SHA-2 within the current time frame established. TSYS has nearly 220 ISVs/VARs impacted by the change to SHA2.
- While the industry can update and remove SHA- 1 from browsers, there is a significant challenge to expedite the removal and replacement of SHA 1 with SHA 2 certificates in payment terminals.

Technical Overview
The following is an illustrative case study for consideration –

- SHA -1 certificate on terminal expires on August 3, 2016
- Terminal may still reside at merchant location
- Terminal contains an expired certificate
- Merchant attempts to accept a transaction, but will be unsuccessful
- Terminal will display a communications error message
- Merchant may be instructed to call Terminal Help Desk
- In certain instances, efforts may be undertaken to provide a terminal software download in an attempt to resolve the matter
- However, terminal downloads typically take anywhere from 20 to 45 minutes to complete
- Terminal Help Desks may be overburdened with massive incoming call volumes causing slower resolution times with merchants placed in a holding patters
- Some terminal software downloads may not suffice as some terminals may not contain enough memory to support the updated certificate
- Merchants may then be required to purchase a replacement terminal which can take numerous days to remedy

Consumer Impact and Disruption to Commerce

- When confronted with this situation, a Consumer will need to determine how they can then pay for their goods/services
- If there is no alternative form of payment at the consumer's disposal (i.e., cash), the merchant will likely lose the sale, as a consumer heads out in search of an alternative merchant
- If, for example, the goods needed were medical supplies, the challenge to the consumer and the disruption to commerce could be significant
- TSYS, as a 3rd Party Processor, has hundreds of Acquirers (Merchant Sponsors), which in turn use a number of variants of POS application and devices from many ISVs/VARs not under TSYS control. These solutions must also be mitigated by the Acquirer and ISVs/VARs to reduce the likeliness of consumer impact.

6. What is the anticipated date the transition from SHA1 Certificates will be complete?

February 09, 2017

7. When, and how did the Subscriber first become aware of the SHA1 sunset?

04/01/2014 - Symantec announces the move to SHA2
04/01/2014 - SHA2 New Chain available by default in Symantec MPKI for all Users
01/16/2015 - TSYS Begins Planning/Testing of Identified Symantec Chain
02/16/2015 - Implementation Sand Box testing begins with SHA2 Chain
08/28/2015 - TSYS Internal announcement sent after successful testing with selected applications
11/30/2015 - Symantec report of remaining SHA1 certs sent internally by TSYS
11/30/2015 - Email notification to TSYS NA Account Management
12/01/2015 - Symantec makes SHA2 full change available
12/08/2015 - TSYS Information Bulletin sent to all clients globally

12/15/2015 - Symantec recommended everyone speed up migration to SHA2 – Shared internally at TSYS
12/23/2016 - Internal notification to Issue Bulletin for POS Devices related to SHA1 certificates
02/01/2016 - Bulletin to TSYS Acquiring clients related to SHA1 certificate End of Support for POS devices/applications
02/01/2016 – Testing and Impact Assessment started for POS applications and devices
02/26/2016 – 2nd Bulletin to TSYS Acquiring clients related to SHA1 certificate End of Support for POS applications and devices

8. What procedures are in place to ensure a similar exception will not be required when standards currently in use are deprecated?

- Improved / Advanced Communications to Clients / Partners across all Payment Services with positive reporting users have received and understand the communications
- Unified Internal Communications and Education Sessions
- Plans to modernize technical solutions (i.e. SHA-3, others) and encourage POS Application / Device Support as early as possible
- Additional Lead Times to Implement Solution from CAs
- Potential Use of Alternate / Private Certificates Signed by a Root CA

9. The number of Requested Certificates

Eight (8) total for Four (4) FQDNs

- ssl1.vitalps.net
- ssl2.vitalps.net
- ssl3.vitalps.net
- ssl1.tsysacquiring.net

10. For each Requested Certificate: Symantec

a. The proposed tbsCertificate in DER format, i.e. the exact bit pattern that would be signed. (Note this could be attached separately and a SHA256 hash of the DER file included in the signed request). The not before date may be up to 14 days in the future to accommodate the review time.
b. A corresponding human readable version, for reference.
c. A crt.sh link to the Existing Certificate.
d. Additional information as required by Existing Certificate Information section.