TRUSTED SECURITY
SOLUTIONS

2016 REMOTE KEY LOADING REPORT

UPDATED AUGUST 2017

The information provided herein by Trusted Security Solutions, Inc., developers of the A98 ATM Initial Key Establishment System has been gathered over time from technical personnel from the various ATM manufacturers listed. This information is accurate and reliable to the best of our knowledge but should not be used as a final determination in planning for remote key loading. The individual ATM manufacturer should be contacted for the most accurate and up-to-date information when determining individual ATM requirements for remote key capabilities.

Encrypting PIN Pads: Out with the old, in with the new!

All ATM manufacturers must have their EPPs (Encrypting PIN Pads) inspected and approved by PCI Security Council's Recognized Laboratories. All existing EPPs for ATMs under the label PCI PTS POI v1.0 (Payment Card Industry PIN Transaction Systems Point of Interaction version 1) fall under an approval that expired April 30th, 2014[1]. It is TSS's understanding that all current EPPs (PCI PTS POI v1.0) are grandfathered – i.e. these EPPs may remain in service indefinitely unless the ATM is moved. Also, these EPPs may be replaced with an "in-kind" EPP as long as the replacement service on the ATM is being provided by the original purchaser.

MasterCard mandated that PCI PTS POI v1.0 EPPs can be "deployed" until April 30, 2014. VISA mandated that this style EPP can be "purchased" until April 30th, 2014.

PCI PTS POI v1.0 EPPs are being replaced with PCI PTS POI v.3.X EPPs. The new EPPs must support public keys with signature hash algorithms (SHA) of 256 bytes. According to the PCI PIN V2 publication published in December 2014, PCI PTS POI v.3.0 EPPs deployed supporting both SHA1 and SHA256 must migrate to SHA256 by December 2016.

In this summary report, we will take a look at the current status of each ATM manufacturer's version of their PCI 3.X EPP and more importantly what impact these new EPPs will have on your business.

With the convergence of PCI EPP 1.X and PCI EPP 3.X EPPs, ATM owners face new challenges in supporting double the number of RKL protocols as before, and knowing when to use which one. To reduce the complications of this change for banks and processors, TSS is not only seamlessly integrating these new 3.X protocols into its core RKL procedures, but also designing intelligence into its processes to automatically use a logical progression of protocols if needed to successfully remote key the ATM.

To learn more about these changes, please contact TSS at info@trustedsecurity.com.

Diebold/Nixdorf

Diebold's new EPP is the EPP7. The EPP7 is backward compatible and uses the same cryptographic process and existing signed certificate as previous versions of Diebold's EPPs - EPP4s and EPP5s. This "migration period" of backward compatibility ends December 31, 2017. At that time Diebold will stop manufacturing EPP7s with support for SHA-1 and deliver only EPP7s with the SHA-256 hash algorithm. ATM owners need to ensure that their remote key process for Diebold EPP7 supports SHA256 before the migration period ends.

EPP4s and EPP5s have used a web portal to Identrus as the Certificate Authority. EPP7 SHA256 key signing requests use a similar portal with Symantec. Ask your Diebold/Nixdorf representative for the latest portal to use in starting the certificate signing request process.

Important Note: Once an EPP7 has been remotely keyed with a host certificate signed using the SHA256 algorithm, it can no longer be used in SHA1 mode.

Decommissioning EPPs: EPP5s and EPP7s enforce the concept of "host binding". These EPPs can be remotely loaded by a host using the same host certificate an unlimited amount of times. If the ownership of the ATM changes such that remote key loading will now be performed from a different host (i.e. different host certificate), or if the original host certificate is replaced with a new one, the EPP will need to be "decommissioned" prior to remote key loading.

The following software releases support EPP7: Agilis 3 91x, SP3, Agilis 3 NDx, SP5, Agilis XFS Version 3.11 or higher, ValiTech 3.3 Agilis® 2.4, patch 11 (not applicable to Diebold North America (DNA)).

Diebold EPP4s, EPP5s, and EPP7s using the legacy and new cryptographic processes and certificates are fully supported by the A98 Remote Key Solution version 5.7 and higher.

VISTA™ Software: TSS has certified remote key loading using VISTA on Diebold ATMs and is presently working to certify VISTA RKL on Wincor ATMs.

NCR

NCR's new EPP is the EPP3. It is backward compatible. No action is required to use the new EPP as an EPP in a newly installed ATM or as a replacement EPP in an existing ATM. NCR offers a new remote keying protocol, named Enhanced Protocol, which is intended to provide compliance with current PCI requirements. Once the EPP has been remotely keyed with Enhanced Protocol, the EPP is locked in Enhanced Mode until the intermediate public key is deleted using "authenticated deletion". Enhanced Protocol is not widely used. Enhanced elements in the protocol are present to prevent replay and bind the ATM to the host.

Future plans. By April 2020 NCR customers will need to have migrated from the legacy NCR signature protocol. NCR has delivered EPP firmware and ATM software that supports TR34 and TR31. Whereas TR34 SHA256 is required starting January 2018, elements of TR31 are not mandated until later times. All EPP's running firmware version INTL_64 and above support TR34. APTRA XFS v6.4.1 and upwards have the correct implementation for both TR34 and TR31.

NCR's Basic Protocol, Enhanced Protocol, and TR34 and TR31 are fully supported by the A98 Remote Key Solution v6.2 and higher.

Wincor Nixdorf

Wincor Nixdorf's migration plan gives customers to ability to migrate at their own speed to the PCI PTS POI v3.X standards All the remote key capable EPPs (EPP J61, EPPv7 and EPPv6) support remote key loading using SHA1. According to information received by TSS, Eppv5 does not support remote key loading. EPPv7 has support for SHA256 but it is not apparent that EPPv6's support SHA256 at this time. For the minimum firmware levels needed to support SHA256 and the time frame for EPP SHA256 support, one should contact Wincor technical support. Using the Wincor Key Exchange/Key Request Form, customers may request signed public keys with either SHA1 or SHA256 signatures.

Wincor Nixdorf's legacy SHA1 is fully supported by the A98 Remote Key Solution v6.0 and higher. TSS is working now with several clients to build support into our 6.2 release for the Wincor SHA256 protocol.

Nautilus Hyosung

Nautilus Hyosung has remote key loading available on certain ATMs. To enable remote key loading the software in Hyosung ATM must be MoniPlus2 version 01.04.05 or higher and the EPP must be one that supports remote key loading.

Nautilus Hyosung's PCI PTC 3.0 EPP is called EPP Version 3.0. When requesting a signed public key from Hyosung, one should ask for specific instructions on how to send and receive the signed key. The minimum software level to support remote key loading for the EPP Version 3.0 is MoniPlus2 02.03.20 (some call it MP2s). If you have Hyosung ATMs in your fleet remotely keyed using the current public keys and SHA1 signature, and you have plans to deploy the EPP8000X, you will need to acquire a new host public key signed by Hyosung's new CA for remote key loading of the new EPP.

Hyosung's remote key loading, using both the old CA and the new CA, are fully supported by the A98 Remote Key Solution version 5.8 and higher.

PCI Bulletin on Expiration of v.1 devices:
https://www.pcisecuritystandards.org/pdfs/14_03_19_PCI_SSC_Bulletin_on_the_expiration_of_the_approval_of_PTS_POI_v1_devices_final.pdf