TRUSTED SECURITY
SOLUTIONS

2021 REMOTE KEY LOADING REPORT

UPDATED JANUARY 2021

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.

New requirements impact the industry. Here's what you need to know:

2021 will be a pivotal year for ATM owners using or considering the use of remote key loading for their ATM fleet.

If you are **not using remote key loading technology**, you are shouldering unnecessary risks and labor costs by using paper components and manual procedures.

Remote key loading is **a powerful tool**. Planning and preparation are key to getting your money's worth.

The start of year 2021 brings us to a confluence of complexities:

AUDITORS ARE ENFORCING USE OF SHA256

- SHA256 was mandated for use January 2017. Non-compliance with "action plans for future implementation" is no longer acceptable in many cases.
- New EPPs (Encrypting PIN Pads) are replacing outdated, non-compliant EPPs. You may not be able to re-order SHA1 EPPs for replacements.
- Plans to adhere to the PCI and VISA's staggered roll out of key bundling mandates (key storage, key transport, and key use in devices) must be in place or in the planning stages, and
- EPP firmware updates are critical to be matched with ATM software and key management schemes, otherwise remote key may not work as expected.

We hope this whitepaper will help guide you on your upcoming decisions about remote key.

Encrypting PIN Pads: A story of constant evolution

PCI PTS POI Compliance

Payment Card Industry PIN Transaction Security Point of Interaction

All ATM manufacturers are required to have their Encrypting PIN Pads (EPPs) inspected and approved by PCI Security Council's Recognized Laboratories. EPPs are submitted to PCI approved labs seeking a specific level of PCI PTS certification. Once approved, the EPP is deemed compliant with that version standard and can be used until the end of the version validity period of that particular PCI PTS version expiration date.

PCI PTS Device approval dates constitutes a line in the sand where any new ATM being sold after that date must have the most current, approved PCI PTS EPP. Existing ATMs installed with earlier PCI PTS EPPs can continue using those EPPs and operate "in compliance" indefinitely. A time will come when you will no longer be able to order replacement PTS v3 EPPs from your ATM manufacturer. ATM owners should have a plan to change PTS v3 EPPs to PTS v5 EPPs for new ATMs, ATMs that have been moved, or ATMs needing a replacement EPP.

In this way, ATM owners will be prepared to upgrade to newer PCI PTS versioned EPPs over time. There is no requirement to upgrade EPPs all at once.

Device validity periods have expiration dates. PCI issues an "end of operation" date for EPPs. For EPPs "pre-PCI", the end of operation date is the end of 2020. For PCI PTS version 1 EPPs the end of operation date is 2022. For PCI PTS versions 3 and above, the end of operation date is currently open ended - no end of operation date is set for PTS v3 EPPs at this time. As a rule, device validity periods expire on April 30th every 3 years. Another way of looking at it is that the validity periods are set up to last for 2 PCI PTS cycles. A key PCI PTS date is fast approaching.

> The device validity period for PCI PTS EPPs under the label PCI PTS v3.0 was to expire on April 30, 2020 but has been extended to April 30, 2021. ATMs purchased after this date must have a PCI PTS v4.0 or higher rating.

What does that mean for PCI PTS v3.0 EPPs?

PCI PTS 3.0 or earlier version devices do not need to be replaced. They can operate compliantly for an indefinite period. Guidance on how long they can operate will come from PCI or the networks in the coming months. Here is a list of PCI PTS version 3.0 and version 5.0 EPPs for your reference:

MANUFACTURER	EPP 3.0	EPP 5.0
Diebold/Nixdorf	EPP7, EPPv6, EPPv7, ETS	EPP 7.5, EPP 8
NCR	EPP3, EPP4 (v3 firmware)	EPP4 (v5 firmware)
Hyosung	PCI 3.0 EPP	EPPX1
Triton	T9	T10
GRG	EPP-003	EPP-004
OKI	HMB9201S	-

If you have detailed questions about your EPPs, contact your ATM vendor to gain the most accurate and up-to-date information.

SHA256

Secure Hash Algorithm 256 bit size

In December 2014, PCI PIN Security Requirements v2.0 mandated the use of SHA256 whenever hash algorithms were used in PCI PTS 3.0 devices for key distribution using asymmetric techniques. The deadline was set for 24 months hence, or December 2016 as the time when SHA256 "must" be used. Remote key loading protocols for ATMs use hash algorithms and specifically SHA-1 prior to this mandate. Since 2014, EPPs have been in varying states of migration from SHA-1 to SHA256.

PCI PTS 3.0 EPPs generally are engineered with a split personality – SHA1 and SHA256. A key point in the PCI PTS 5.0 requirements is that the EPP can only use SHA256 and cannot be engineered to be backward compatible to SHA1.

When migrating your PTS v3 SHA1 EPP to SHA256 status, successfully implementing SHA256 depends one of more of the following:

- if the processing host has the capability to use SHA256,
- if the EPP has firmware to support SHA256, and
- if the EPP is properly configured to use SHA256
- if the EPP can be "unbound" from the previous RKL Host

More information will follow on status of SHA1 to SHA256 for each manufacturer in the remaining parts of this report.

TR-34/TR-31

Technical Report 34/Technical Report 31

Q: What is TR-34?

A: TR-34 describes a method consistent with the requirements of ANS X9.24 - 2 Retail Financial Services Symmetric Key Management - Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys for the secure exchange of keys using asymmetric techniques between two devices that share asymmetric keys. To quote ANSI 2: "This method is designed to operate within the existing capabilities of devices used in the retail financial services industry."

NCR was the first to incorporate the use of TR-34 for the delivery of the master key to the EPP during remote key loading. Many other ATM manufactures are also adopting the use of TR34 as an option.

The following pages will include additional information about specific EPPs by ATM manufacturer and if they currently support TR-34 or not or if they have published plans to do so.

Q: What is TR-31?

A: TR-31 is a method consistent with the requirements of ANS X9.24 Retail Financial Services Symmetric Key Management Part 1 for the secure exchange of keys and other sensitive data between two devices that share a symmetric key exchange key. This methodology is being adopted for storage and transmission of symmetric keys. There are different versions of TR-31 keys (ie. TR-31 version A, TR-31 version C, etc.). HSM manufacturers often have their own proprietary versions of key blocks. The differences from one version to the next depends on the intricacies of the format and encryption used. TR-31 version B (TR31B) is the most commonly used TR-31 key block. TR-31D utilizes AES encryption and is viewed as the most secure.

On the following pages, read how each ATM manufacturer is dealing with these complex decisions.

Diebold Nixdorf

Diebold Nixdorf's most widely distributed EPP in use today is the EPP7. The EPP7 is PCI PTS v3 compliant and is backward compatible to operate much like the EPP5. It uses the same SHA1 cryptographic processes as the EPP4 and EPP5 so the existing signed host certificates for previous versions of Diebold Nixdorf's EPPs - EPP4s and EPP5s – will work to rekey the EPP7 in SHA1 mode.

The EPP7 can also be configured to use SHA256 certificates.

When migrating an EPP7 from SHA1 mode to SHA256 mode, the normal scenario would be for a Diebold Nixdorf technician to visit the ATM, decommission the EPP with a secure token to "unbind" the EPP from the previous SHA1 host certificate, configure the EPP to use SHA256 certificates, then have a new remote key loading operation performed using the new SHA256 host certificates.

TSS has experienced varied results during this migration. Based on TSS's experiences, once your ATM driving host is loaded with signed SHA256 certificates from Diebold Nixdorf's Certificate Authority, TSS suggests:

- Test a rekey without any changes to the ATM using the new SHA256 certificates. If a rekey in this scenario does not work, you may get a REJECT response during the RKL sequence from the ATM.
- If you receive a REJECT response, have the EPP decommissioned, either by a Diebold Nixdorf service technician with his/her security token or by using remote decommissioning commands. The remote decommission will only work if you use the same SHA1 certificates that were used to remote key load the EPP previously.

Some of the variables that TSS has found significant during SHA256 migrations are:

- The EPP settings in the ATM configuration tables should be set for SHA256 whenever possible
- The XFS layer must be compatible with the version of ATM driving application software in use on the ATM.

- If you have EPP setting options for “Basic” or “PCI”, and you are having issues, you should change this option to see if it makes a difference. A setting of “PCI” is more secure.

Diebold Nixdorf targeted April 2020 to suspend shipments of PCI PTS v3 EPPs – the EPP7. Due to the COVID pandemic, this deadline was moved forward. Diebold Nixdorf will soon start shipping exclusively the EPP7.5 and EPPv8’s instead. Contact Diebold Nixdorf for exact dates.

Furthermore, Diebold Nixdorf terminated the Identrus SHA1 CA in 2020. Diebold Nixdorf customers will no longer be able to apply for Identrus SHA1 CA signed host certificates. And Diebold Nixdorf has a limited supply of EPPs using Identrus SHA1 CA certificates in stock. For special situations where a Diebold customer must continue using SHA1, Diebold Nixdorf has offered a new SHA1 CA signing service that will work in certain EPPs available from Diebold Nixdorf. For more information, contact Diebold/Nixdorf and ask for additional information.

All signed SHA1 host certificates now in place will continue to work to rekey EPP5 and EPP7s. A particular host certificate may have a certificate expiration date that is either past due or soon to be past due. In this case, the signed host certificate will continue to function normally unless the host has certificate expiry date detection and automatically terminates its use.

The EPP7.5 product announcement states that the EPP7.5 supports native Certificate Remote Key Loading (CTRL) SHA256 & TR-34 Remote Key Loading. If your ATM driving host currently has a signed SHA256 host certificate from Diebold Nixdorf’s CA, you can continue using those signed public keys (host certificates) with EPP7.5’s. If you desired to implement TR34 Remote Key Loading, you would need to apply to Diebold Nixdorf to acquire a new set of signed public keys (host certificates) compatible with TR34.

It is noteworthy that the EPP7, EPP7.5 and EPPv8 will also support the distribution of PIN Encrypting Keys (PEKs) and other session keys using TR-31 version A, B, and C key blocks. Version D to be supported at a later date.

Diebold Nixdorf EPP4s, EPP5s, EPP7s, EPP7.5s, and EPP8s using native CRKL cryptographic processes and certificates are fully supported by the A98 Remote Key Solution version 5.7 and higher

for both SHA1 and SHA256. Additionally, it is important to note that the A98 Remote Key Solution incorporates remote decommissioning.

TSS has certified SHA1 and SHA256 CRKL using Network Solution (Vista) and Agilis on Diebold and Wincor ATMs.

NCR

NCR's latest EPP is the EPP4. The EPP4 is widely used at the PCI PTS v3 approved level and can be brought forward to PCI PTS v5 certified level with PCI PTS5 firmware.

EPP4's can use SHA1 or SHA256 for remote key loading. NCR's position is to allow the customer to make their own decision whether or not to implement SHA1 or SHA256. Customers wishing to be SHA256 compliant will want to install the latest ATM software to make sure that the latest PTS v5 firmware is loaded into the EPP4.

NCR ATM owners wishing to use SHA1 Basic Protocol can continue to apply for and receive SHA1 signed host public keys. When requesting SHA1 signed host public keys, the person completing the form must check a box saying that they are aware that SHA1 is "non-compliant".

If you are an NCR customer using SHA1 remote key loading today, you drive your own ATMs, and you wish to be PCI compliant and migrate to SHA256, you must contact your local NCR representative, complete the NCR key signing form request, and transmit your new public key with a SHA256 hash for CA signing. The key signing process for SHA256 is similar to the process for SHA1.

Migration to SHA256 may require software and firmware upgrades. INTL_65 EPP software is PCI PTS version 3 and PTS version 5 compatible. GLBL_ EPP software is strictly PCI PTS version 5 compliant (ie. no backward support for SHA1). If you have INTL_65 firmware, you are able to configure and use either SHA1 or TR34 SHA256 during remote key loading. If you have GLBL_ EPP firmware, you can only use SHA256.

When implementing the use of SHA256, you must determine the transport mechanism of your session keys based on the capabilities of your host ATM driving software. Is your transaction host capable of transporting session keys using TR31? Based on the answer to this question, consult your NCR and host technical support teams to architect the message flow for RKL.

Important Update! SHA256 compliance is now possible for most NCR users!

If you wish to use TR34 "uncoupled" from the use of TR31 keyblock delivery of the PIN key, you are now able to do this with the latest software and firmware updates from NCR. Get with your NCR representative to receive these updates and start using TR34 (SHA256) for loading your ATM EPP with Terminal Master Keys and continue to use TDES to load your PIN keys.

Diebold/Nixdorf (legacy Wincor ATMs)

From a key management standpoint, remote key loading processes for legacy Wincor ATMs remain the same. The Certificate Authority for Wincor legacy ATMs remains in Diebold/Nixdorf's offices in Germany. Use your Diebold/Nixdorf representative to sort out procedures for public key signing.

EPPv6, EPPv7, ETS, and EPPv8 all support SHA1 and SHA256 and are PCI PTS version 3 certified. Only the EPPv8 with appropriate firmware is PCI PTS version 5 certified.

To support standard SHA256, obtain the key request forms from Diebold/Nixdorf pertaining the your EPPs and follow the process to submit the forms specifying that you wish to have SHA256. You should receive back signatures for your public key and some additional bin files. The public key signature will need to be imported into your host software. The bin files will need to be loaded onto your ATMs.

You are able to request either a Test, Pilot, or Production public key signature from Diebold/Nixdorf for your legacy Wincor ATMs. If you do not have a Test EPP, we suggest that you request a Pilot and

Production key to use in performing RKL tests and migrating onwards to production. EPP serial numbers will be required when requesting signed public keys. The serial number labels can be found on the back of the physical EPP.

The EPPv8 is PCI PTS v5 approved and uses SHA256 during remote key loading. It is also slated to support TR34 CRKL like the EPP7.5.

TSS has certified SHA1 and SHA256 remote key loading with Wincor ATMs.

Triton

Below is a list of the Triton EPPs and their remote key characteristics:

- The Triton T-5 EPP is remote key capable and supports SHA1.
- The Triton T-9 is PCI PTS Version 3 certified and is exclusively SHA1
- The Triton T-10 is PCI PTS Version 5.1 certified and is exclusively SHA256.

The Triton remote key loading process is a certificate-based protocol that uses Triton specific schemes to bind the ATM to the host and reduce the risk of “replay”.

Triton’s T5, T9, and T10 EPPs are fully supported by the A98 Remote Key Solution version 5.8 and higher. The Triton T10 EPP has been certified with the A98 using SHA256.

According to information received from Triton, these ATM models: ARGO 7/12/15/FT, Traverse, RL1600, RL2000, RL5000, FT5000, RT2000, will support SHA 256 as long as they have a T10 keypad using 4.2.1.11 software or higher.

Hyosung

The Hyosung PCI PTS version 3 EPP is the EPP8000 EPP. The EPP8000 model supports both SHA1 and SHA256. The EPP8000 supporting SHA1 has a different part number that the EPP8000 SHA256 version. There is not a version of the EPP8000 that supports both SHA1 and SHA256.

The Hyosung PCI 5.0 EPP is the EPPX1. The EPPX1 only supports SHA256.

If you have previously acquired a signed SHA256 host public key from Hyosung's CA, that signed public key will work both on SHA256 EPP8000 EPPs as well as the EPPX1.

Hyosung retail ATMs use Hyosung's proprietary MoniPlus software and the financial ATMs uses software supporting NDC messages.

When requesting a signed public key from Hyosung, you 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 (MP2). If you have Hyosung ATMs in your fleet remotely keyed using a SHA1 signature, and you have plans to deploy the EPP8000X (SHA256 version) or EPPX1 to implement SHA256, you will need to acquire a new host public key signature from Hyosung's new CA for remote key loading of the new EPP.

The SHA1 EPP8000 and the SHA256 EPP8000 PCI 3.0 EPP is fully supported by the A98 Remote Key Solution. The EPPX1 is also fully supported by the A98 Remote Key Solutions and has been certified by TSS and several TSS customers.

GRG

The GRG EPP-004 supports SHA1 and SHA256 and is fully supported by the A98 Remote Key Solution. To use SHA256 you must have EPP firmware version 1.03 or higher. GRG's PTS version 5 EPP is the EPP-004A and it supports SHA256 only. The EPP-004A is currently only available outside the US but a PTS PCI version 5 model for the US is due out soon.

The GRG SHA1 and SHA256 remote key protocols have been successfully tested by A98 customers and is fully supported by the A98 Remote Key solution.

OKI

TSS has successfully remotely loaded keys into OKI ATMs in the past using SHA1 and most recently successfully certified SHA256. A98 supports remote key protocols for OKI ATMs using the HMB9201S EPP.

Ready to learn more?

Each remote key loading installation is different. TSS is knowledgeable of all current standards and ATM vendor specifics. We are available to answer questions about RKL for your ATM fleet. Visit www.trustedsecurity.com or contact us at info@trustedsecurity.com for more information.

1. 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
2. ANSI websites:

   TR-34

   https://webstore.ansi.org/Standards/ASCX9/ASCX9TR342019

   TR-31

   https://webstore.ansi.org/Standards/ASCX9/ASCX9TR312018

   Complete pack of X9.24-1, -2, and TR-31

   https://webstore.ansi.org/Standards/ASCX9/ANSIX924ASCTR31SymmetricKey

TRUSTED SECURITY SOLUTIONS