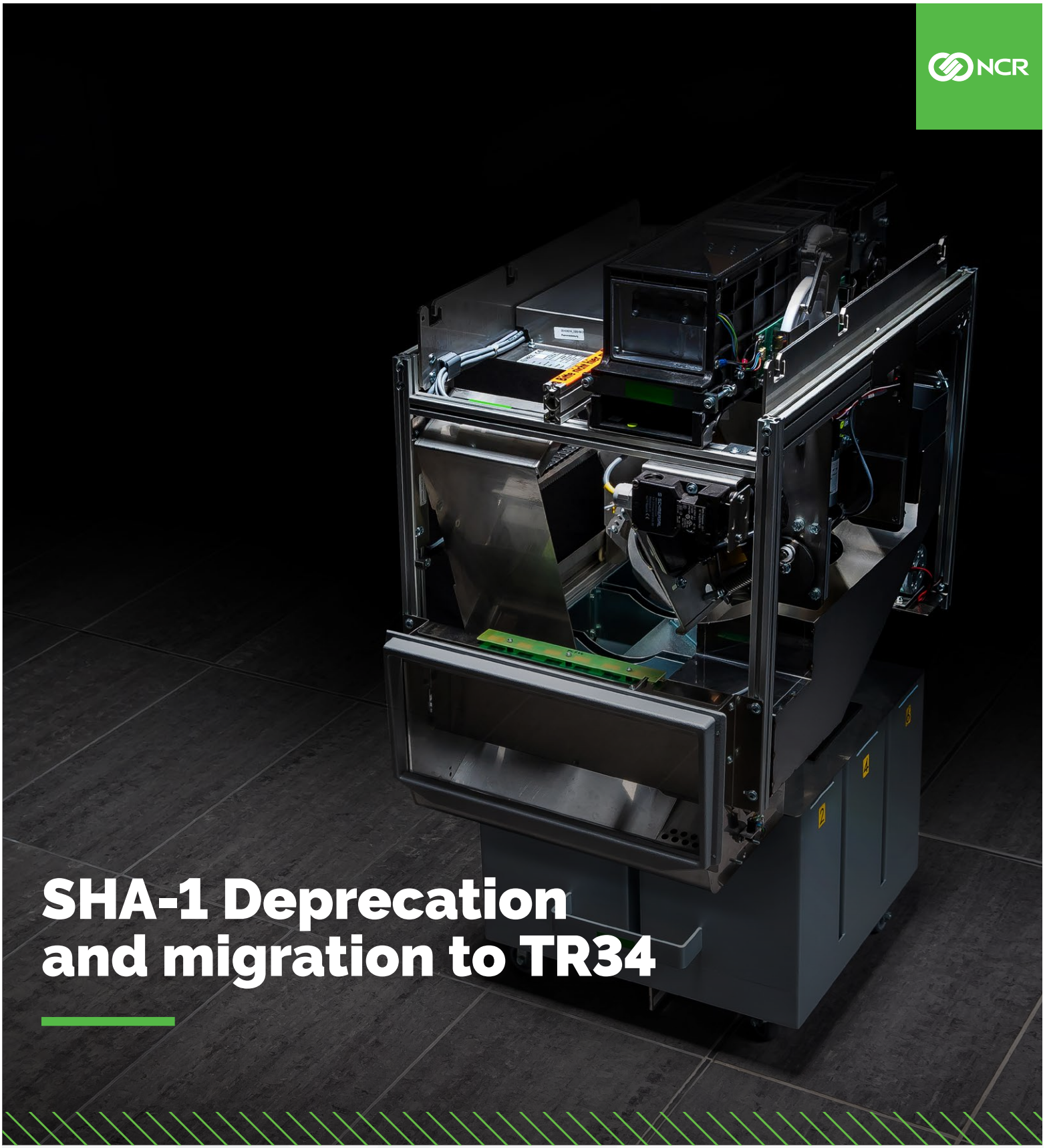

SHA-1 Deprecation and migration to TR34

NCR security white paper

May 2022. REV 1.3

SHA-1 Deprecation and migration to TR34 Summary

In 2011, NIST deprecated the SHA-1 hashing algorithm, used in ATM Remote Key Distribution systems; it has been disallowed for use by PCI PIN since 2017. On **April 30, 2021**, PCI PTS will disallow support for SHA-1 in new, compliant EPP deployments. If you're an NCR Remote Key customer, you should have plans in place to migrate to TR34—NCR's Remote Key protocol that uses SHA-256—before this date to maintain your future PCI PTS compliance.

NCR currently has no plans to discontinue support for SHA-1. All SHA-1 systems will continue to function during this migration period.

Timetable: PCI PTS V3 expiration date extended

Due to the global impact of the coronavirus, PCI has extended the expiration date of PTS V3-approved devices to April 30, 2021. This extension doesn't change any PCI compliance rules; it's simply a change of date.

That means, if you want to maintain PCI PTS compliance for future ATM deployments, you MUST complete migration to TR34 BEFORE April 30, 2021.

Will PCI issue new certificates with the new expiration date?

No. The PCI website, www.pcissc.org, has been updated with the new date. You should always check PCI PTS compliance against the website, not the paper certificates—the website always has the most up-to-date information.

What is TR34?

TR34 is an industry standard, interoperable method for remotely keying an ATM and is written by Accredited Standards Committee X9 for use in the financial industry. You can get copies of the TR34 document from the Standards Store at www.X9.org.

TR34 is listed as a PCI PIN compliant method of Remote Key Distribution in version 3 of the PCI PIN specification. Use of TR34 simplifies the PCI PIN audit process because you no longer have to justify how a proprietary method of RKM meets the requisite security controls of PCI PIN.

The TR34 key exchange process is similar in principle to the original NCR implementation of Remote Key Management, although the formats of the certificates and messages are different, and additional security controls have been included in the protocol.

What is required to migrate to TR34?

TR34 is a protocol that's operated between the host key manager HSM and the EPP in the ATM. That means you have to update all layers of software in the path of that key transport flow to be compatible with TR34. This means:

- EPP firmware
- XFS platform software
- ATM application software
- Terminal handler software
- Host HSM firmware and;
- You need to request a new certificate from NCR for a TR34 Key Distribution Host certificate. Please see document "**NCR TR34 Key signing process**" for details on how to request a KDH certificate for TR34.
- EPP4 test kits. These are useful for development of TR34 systems. The test kit is an EPP4 loaded with non-production keys, which means there's no need to maintain security controls with this device. This simplifies the development and debug activities by removing the need for security. We recommend using the test kit, but it's not mandatory. For customers who decide to use the test kits, please allow for delivery lead time in TR34 project plans. The test kit has accompanying instructions and test data. You can request this information from Solution Information Services at SolutionInformation.Services@ncr.com or from Solution Management.

Which EPPs support TR34?

Most of NCR's EPPs will support TR34 with an appropriate firmware update. NCR has been loading SHA-256 certificates into our EPPs since 2012, so only some older EPP2s and Personas ATMs can't support TR34. See Appendix A of this document for a list of NCR EPPs and their capabilities.

Which firmware version do I need to support TR34?

For EPP4, the version of firmware you'll need for TR34 is either GLBL_01, or INTL_81. Note, however, that GLBL_01 is approved to PCI PTS V5 and will become necessary for compliance in new deployments after April 30, 2021. INTL_81 also supports TR34, but INTL_81 is approved to PCI PTS V3, and therefore should *not* be used for new deployments after April 30, 2021.

How is EPP firmware managed?

The APTRA XFS platform manages EPP firmware. This means there's no requirement to install specific EPP hardware to get the functionality necessary for TR34. Please see **NCR SECURITY ADVISORY—EPP4 V1.1** for full details.

Can I still order EPP3 now that the expiration date has been extended?

No. NCR has discontinued EPP3 in line with the original expiry date for PTS 3. NCR no longer has stocks of parts that would be necessary to manufacture EPP3, and the EPP3 secure microprocessor and a memory component are now obsolete and EOL.

Is there any requirement to upgrade hardware?

No. PCI PTS requirements only apply to future deployments. Upgrades would only be required if you want to deploy TR34 across your entire installed base, and some of the base are older EPP2 or Personas ATMs. In that case, the EPP2 can be upgraded to EPP4. There is no EPP upgrade for Personas family ATMs, and NCR recommends that you replace the ATM with a modern model.

How can I identify the EPP type?

You can identify EPPs by a combination of model, hardware ID and firmware version. EPP2, EPP3 and EPP4 are actually NCR nicknames for the different generations of the 5815 model EPP. The simplest way to identify an EPP is to look at the hardware ID. EPP4 all have a hardware ID of 009-0031480; all EPP3 have a hardware ID of 009- 0028973. EPP2 have a variety of hardware IDs, so please see the list in Appendix A at the end of this document.

Is manual key entry affected by this these changes?

No. EPPs retain the option of having the initial master key entered as a minimum of two full-length components typed on the EPP keypad. This function is known as 'Secure Key Entry' and the interface doesn't change with the introduction of EPP4 with PCI PTS V5 compliance.

Do SHA-1 certificates have an expiration date?

No.

If PCI PIN banned SHA-1 in 2017, why can PCI PTS V3 devices support SHA-1?

It's because there are two different PCI programs that govern PIN security: PCI PTS and PCI PIN.

PCI PTS dictates the security requirements for the devices sold by manufacturers like NCR. Manufacturers are responsible for ensuring the device is complaint and approved. Customers can verify PCI PTS compliance by looking for the listing on the PCI SSC website.

PCI PIN dictates how an organization should manage its cryptographic infrastructure, and this covers key management, device management, processes and procedures. This can lead to situations where compliant devices may support functionality that PCI PIN outlaws. SHA-1 is one example.

PCI PTS-approved devices are permitted to support both SHA-1 and SHA-256; however, from 2017, PCI PIN has dictated that SHA-1 should not be used in those devices.

Another example is key blocks in PTS V5-approved devices. PTS V5 devices are permitted to support both key block and non-key block technology. But from June 2023, PCI PIN will outlaw use of non-key block technology in ATM EPPs.

If you have any questions or need additional information, please contact your NCR Account Manager.

Appendix A

EPP Name	PCI PTS Identifiers			Generation	ATM family	Manufacturer	PCI PTS approval	Approval Expiry	SHA-1 Support	SHA-2 Support	Key Block Support	Upgrade Path	Sunset Date
	EPP Model	HW version	FW version										
Hi-Sec EPP	5807 / 5814	009-0019322 HO5005 009-0028041 445-0748310	6.20 7.08 7.10 7.53 7.54 9.04 9.08 9.53	First	Personas	Hypercom / Verifone Spares since 2014 - NCR	PTS 1.0	30-Apr-14	Yes	No	No	None	31-Dec-22
UEPP2	5815UEPP	009-0023899 009-0023900 009-0024164 009-0024165 009-0024379 009-0024380	INTL_17 INTL_20 INTL_25 INTL_58 INTL_59 INTL_61 NTL_64xxxxxx FRA 15 FRA 17 SWI 12 SWI 14 BDB 02	Second	Self Serv)	Hypercom / Verifone	PTS 1.0	30-Apr-14	Yes	No	No	EPP4	31-Dec-22
UEPP2 (Serial number 02650000 and above)	5815UEPP	009-0027344 009-0027345 009-0027689 009-0027690	INTL_58 INTL_59 INTL_61 INTL_64xxxxxx FRA 17 SWI 14 BDB 02	Second (NCR made)	Self Serv	NCR	PTS 1.0	30-Apr-14	Yes	Yes TR34, upgrade firmware to INTL_64	Yes TR31, upgrade firmware to INTL_64	EPP4	31-Dec-22
EPP3	5815 EPP	009-0028973	INTL_61 INTL_62 INTL_63 INTL_64xxxxxx INTL_65xxxxxx SWI 13, SWI 14 FRA 17	Third	Self Serv	NCR	PTS 3.0	30-Apr-21	Yes	Yes, TR34	Yes, TR31	EPP4	31-Dec-30
EPP4	5815 EPP	009-0031480	INTL_80xxxxxx INTL_81xxxxxx FRA 80xxxxxx GER 40xxxxxx	Fourth	Self Serv	NCR	PTS 3.0	30-Apr-26	No	Yes, TR34	Yes, TR31	XFS upgrade	None
EPP4	5815 EPP	009-0031480x (where x = blank, S or P)	GLBL_01xxxx	Fourth	Self Serv	NCR	PTS 5.0	30-Apr-26	No	Yes, TR34	Yes, TR31	XFS upgrade	None

Contact us at NCR.com today

About NCR

NCR Corporation (NYSE: NCR) is a leading software and services-led enterprise provider in the financial, retail, hospitality, small business and telecom and technology industries. We run key aspects of our clients' business so they can focus on what they do best. NCR is headquartered in Atlanta, GA with 34,000 employees and solutions in 141 countries. NCR, and SelfServe are trademarks of NCR Corporation in the United States and other countries.