HYOSUNG

ATM Security

PCI Compliance Update

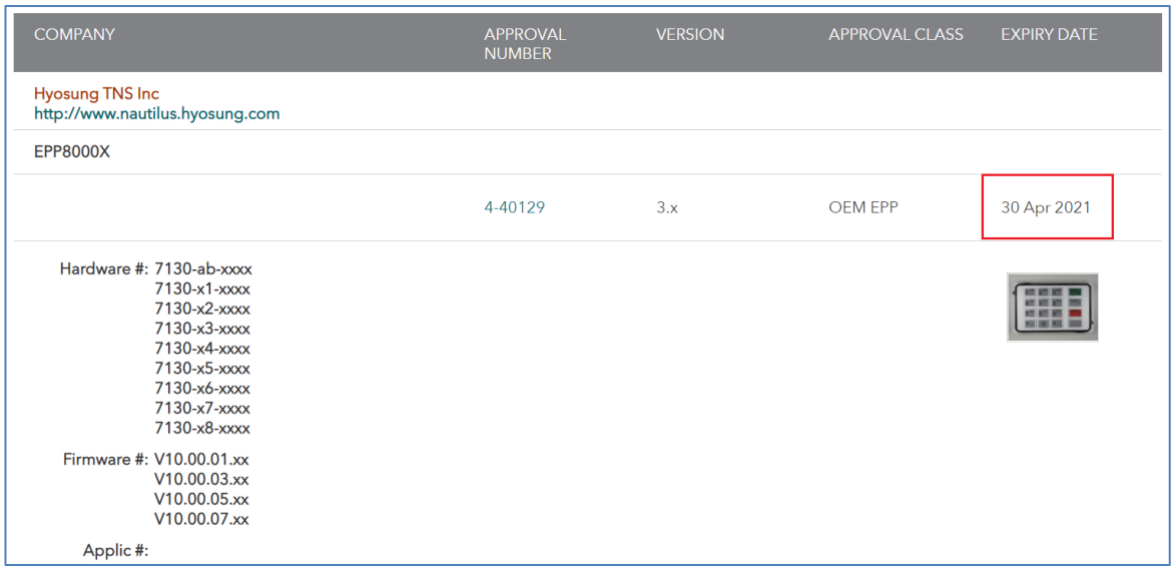
PCI PTS v3 and SHA-2 Transition

PCI PTS v3 is approaching the end of life

PCI Security Standards Council (PCI SSC) extended the PCI PIN Transaction Security Point of Interaction (PTS POI) v3 device's expiration date for one year. The v3 standard was originally planned to expire on April 30, 2020. However, on March 10, 2020, the SSC announced a one-year extension due to the COVID-19 related circumstances.

April 30, 2021

Accordingly, the PCI SSC website will show the Hyosung's EPP8000X devices under the v3 category until the expiration date.



COMPANY	APPROVAL NUMBER	VERSION	APPROVAL CLASS	EXPIRY DATE
Hyosung TNS Inc http://www.nautilus.hyosung.com				
EPP8000X				
	4-40129	3.x	OEM EPP	30 Apr 2021
Hardware #: 7130-ab-xxxx 7130-x1-xxxx 7130-x2-xxxx 7130-x3-xxxx 7130-x4-xxxx 7130-x5-xxxx 7130-x6-xxxx 7130-x7-xxxx 7130-x8-xxxx				
Firmware #: V10.00.01.xx V10.00.03.xx V10.00.05.xx V10.00.07.xx				
Applic #:				

The extension of PCI PTS v3 implies you can purchase and install new v3 devices until April 30, 2021. And the PTS v3 devices purchased before the expiration date can be deployed as long as they are PTS v3 compliant.

Unlike other PCI PTS versions, the lifetime of the PCI PTS v3 has conveyed a unique transition regarding the Secure Hash Algorithm (SHA) used for the Remote Key Loading (RKL). Financial institutions that utilize the RKL method must transition from SHA-1 to SHA-2 to comply with PCI PTS and PCI PIN security standards.

SHA-1 is becoming obsolete

Remote Key Loading (RKL)

RKL is well-known around the world as an effective and secure method for master key management. Hyosung's ATM products, encryption PIN pad, and ATM application support remote key loading, following the RKL industry standard. The standard public-key mechanisms use the Secure Hash Algorithm (SHA), one of this article's primary subjects.

SHA-1 versus SHA-2

SHA-1 has become more vulnerable to attacks. The early-adaptor industries have begun eliminating SHA-1, using SHA-2 only—256-bit hash function. During 2014, PCI SSC also began mentioning the SHA-2 requirement in PCI PIN approvals and allowed its members to transition from SHA-1 to SHA-2 over the lifespan of PCI PTS v3 devices.

Hyosung's PCI PTS v3 and SHA-2

As the financial industry prepares for the end of life of PCI PTS v3, it begins to eliminate SHA-1 if the transition has not been completed yet.

Hyosung, a PCI PTS v3 device provider, began SHA-2 support on its v3 devices in 2017.

The following summarizes Hyosung's PCI PTS v3 devices and SHA-2.

- Hyosung's EPP8000X devices are listed in the PCI PTS v3 category. Initially, the v3 devices supported SHA-1 only.
- SHA-1 has been gradually discontinued by the financial industry. Hyosung released SHA-2 support for the PCI PTS v3 devices with the new firmware version v10.00.07.xx. The PCI SSC website enlisted the firmware version in April 2017.
- Hyosung has discontinued supporting SHA-1 from the PCI PTS v5 devices.

Using v10.00.07.xx for SHA-2

As stated above, the EPP8000X model with the PCI PTS v3 compliant firmware v10.00.07.xx supports the SHA-2 RKL environment.

To use this version, Hyosung installs the firmware v10.00.07.xx and securely injects the

SHA-2 signature into the EPPs. The financial institutions can use this version of EPP for the new ATM installations or relocations until April 30, 2021, and the RKL environment will be PCI v3 compliant.

Using the bridging plan

Hyosung lays out the bridging plan in which financial institutions can transition from SHA-1 to SHA-2 using Hyosung's PCI PTS v3 devices (EPP8000X).

The bridging plan's primary aim is to provide an option by which financial institutions can maintain the dual portfolio during the transition to SHA-2. EPP provider Hyosung can replace the deployed EPPs with the v10.00.07.xx EPPs before the financial institutions' backend is ready for SHA-2. When the financial institutions are ready, they can gradually switch to SHA-2 mode over the Hyosung EPPs per their plan.

Bridging plan for the SHA-2 transition

The table below shows Hyosung's EPP models and the associated PCI PTS versions.

EPP model	PCI PTS	Firmware	PCI expiration	SHA-1 support	SHA-2 support
EPP6000X	PTS v1	v07.20.xx.xx v07.21.xx.xx v08.20.xx.xx v08.21.xx.xx	30 April 2014	O	X
EPP8000X	PTS v3	v10.00.01.xx v10.00.03.xx v10.00.05.xx	30 April 2021	O	X
	PTS v3	v10.00.07.xx	30 April 2021	O	O
	PTS v3	v10.00.11.xx	30 April 2021	X	O
EPP-X1	PTS v5	v15.00.01.xx	20 April 2026	X	O

Note: While the firmware v10.00.07.xx can handle either SHA-1 or SHA-2, the running mode is dependent on whether the device has an SHA-1 or SHA-2 signature injected. Currently, the deployed EPP8000X devices have a single signature injected.

Note: The v10.00.11.xx (in blue) is the bridge firmware to migrate from SHA-1 to SHA-2

Scope

As highlighted above, this section refers to the EPP8000X (SHA-1) and PTS v3 devices already deployed in ATM networks. New deployment in the SHA-2-supported networks is not in the scope of this section.

Concept change

The original concept with EPP8000X devices is to have either SHA-1 or SHA-2, not both physically in the device. However, the new plan allows two injections for SHA-1 and SHA-2 digital signatures in the EPP8000X devices.

Procedures

The table below describes Hyosung and financial institutions' (FI) procedures that

prefer to prepare the SHA-2 transition with Hyosung's v3 EPPs before rolling out Hyosung PCI PTS v5 EPPs.

HW procedures	Firmware procedures	FI procedures	SHA
EPP8000X (SHA-1 + SHA2): Install PCI PTS v3 firmware v10.00.07.xx. In the key injection facility, Hyosung injects SHA-1 **and** SHA-2.		If needed, certify the PCI PTS v3 approved firmware v10.00.07.xx on the EPP8000X (SHA-1 + SHA-2).	1
Field service: Service engineers replace EPP8000X (SHA-1) with the new one, EPP8000X (SHA-1+SHA-2). It will run in the SHA-1 mode by default.	**The bridge firmware**: Hyosung develops the new bridging firmware, **v10.00.11.xx**. PCI SSC approves the firmware under the PCI PTS v3 category.	The SHA-2 migration for the back end (HOST) is in progress.	1
		Certify the new PCI PTS v3 firmware v10.00.11.xx.	1
	On downloading, EPP8000X (SHA-1 + SHA-2) will run as SHA-2 mode. SHA-1 will be deleted.	Download the bridge firmware, v10.00.11.xx to EPP8000X (SHA-1 + SHA-2).	1 ▼ 2

Procedure summary:

- Hyosung injects SHA-1 and SHA-2 signatures to EPP8000X devices using PCI PTS v3 compliant firmware v10.00.07.xx; swap current field EPP8000X devices with dual signature versions.
- Hyosung and PCI prepare delta certification for v10.00.11.xx; financial institution prepares SHA-2 migration for the backend.
- The financial institution remotely downloads v10.00.11.xx to EPP8000X devices to force SHA-2 signature usage.

Beyond April 2021, EPP-X1 rollout

Hyosung will be rolling out EPP-X1 on the newly manufactured ATMs after April 30, 2021.

EPP-X1 model acquired PCI PTS v5 certification in October 2019, and it is recommended early EPP-X1 deployment before PCI PTS v3 expires.

If any FI considers using Hyosung's bridging plan for the network's SHA-2 transition utilizing EPP8000X v3 devices, we suggest you contact your Hyosung account representative.