PA-DSS Implementation Guide

PayEx Nordic Payment v1.1.x

Version: **1.8** (Release)

Revision History

Ver.	Name	Date	Comments
1.0	JTK (CT)	2016-11-01	Final QA and release
1.2	JTK	2018-03-04	Minor updates, updated the data flow diagram with BLE
1.3	JTK	2018-04-16	Updated the version number to 1.1.x, updated terminal models
1.4	JTK	2018-05-02	Updated during PA-DSS revalidation 2018
1.6	JTK	2018-05-23	Misc. clarifications
1.7	JTK	2018-10-02	5.4: Clarified suspected compromise procedure
1.8	KLI	2021-04-22	Update chapter 4 table of PTS devices with iUP2xxLE
1.9	KLI	2021-06-24	Update 5.12 with new DNS names
1.10	KLI	2021-10-01	Remove PTS device iCT2xx as it's no longer supported

Reference:

N	Title	Version
1	PA-DSS Requirements and Security Assessment Procedures	3.2
2	SDI Interface specification	3.1

Table of contents

1. Acronyms

C	
CHD	Cardholder Data (PAN, Expiration Date, Cardholder Name and Service Code)
E	
ECR	Electronic Cash Register
P	
PIN Block	A cardholder's encrypted PIN
S	
Sensitive Authentication Data (SAD)	Magnetic Stripe Data, CVV2 and PIN

2. Purpose

PCI SSC (the Payment Card Industry Security Standards Council) was founded by American Ex- press, Discover, JCB, MasterCard and Visa in 2006. Everyone who processes card transactions mustdo so per the security requirements set forth by PCI SSC.

Every merchant who accepts card payments is required to be PCI Data Security Standard compliant. This document describes how to operate the PayEx payment application in a PCI DSScompliant environment, so that the merchant's PCI DSS compliance is not jeopardized.

The PCI Payment Application Data Security Standard (PA-DSS) is a set of security requirementsand assessment procedures which aims to ensure that payment applications are developed and operated in a PCI DSS compliant way.

As a vendor of a payment application, it is the responsibility of PayEx that the payment applicationis PA-DSS validated. It is the merchant's responsibility to comply with PCI DSS requirements.
Resellers of the PayEx payment application, integrators and merchants' system administratorsshould read this document.

This implementation guide covers the requirements of PA-DSS v3.2. to PayEx Nordic Paymentv1.1.x application.

For more information on the PCI standards, visit http://www.pcisecuritystandards.org

3. Implementation guide lifecycle

In order to address PA-DSS Implementation Guide requirements, PayEx maintains a process to re-view this PA-DSS Implementation Guide at least annually and upon changes.
This PA-DSS Implementation Guide will also be reviewed and updated whenever a change to thePA- DSS requirements will occur.
The revision history of this document contains indications about when changes occurred and a briefdescription of the reason for the update.
This document is shared with all existing customers/resellers/integrators through a public web portal(PIM) once updated and approved and it is part of standard documentation delivered with the soft- ware.

4. Application Description

PayEx Nordic Payment application is a payment application for PCI PTS certified EMV terminal hardware. The application uses certified kernels provided by the terminal manufacturer to processEMV chip, contactless cards and Mag Stripe.

CHD are encrypted by secure module, provided by the hardware vendor, after card reading. During pin entry, the secure module has control over the keyboard, and the application never seesthe clear text pin.
No clear sensitive card data (such as track data, card verification codes, PINs, or PIN blocks) arestored on the terminal.

Certified Hardware terminal models used by the application:

Vendor	PTS Device	Approval Number
Ingenico	IWL2xx	4-20181
Ingenico	iPP3xx	4-20184
Ingenico	iPP3xx	4-30176
Ingenico	iSMP	4-20183
Ingenico	iSMP3	4-30175
Ingenico	iUP2xx	4-30075
Ingenico	iUP2xxLE	4-30251
Ingenico	iUR2xx	4-30083
Ingenico	iUC15x	4-30172
Ingenico	iSMP4	4-30220

5. Treatment of Sensitive Authentication Data (SAD) and Cardholder Data(CHD)

5.1. SAD and CHD must be protected

Sensitive Authentication Data(SAD) includes:
- Full track data(magnetic-stripe data or equivalent on a chip)
- CAV2/CVC2/CVV2/CID.
- PINs/PIN blocks.

Cardholder Data(CHD) includes:
- Primary Account Number(PAN).
- Cardholder name.
- Expiration date.
- Service code.

Previous versions of the payment application have never stored these data.

CHD and SAD are transmitted through the merchant's network in encrypted form, and cannot be accessed in the clear by the terminal operator or the ECR. The PIN code itself is inaccessible in theclear even by the PayEx terminal application.

Sensitive authentication data must not be stored after the authorization, *even if encrypted*. Theterminal itself does not retain such data after authorization. Therefore, merchant traffic logs must not include the actual contents of authorization messages sent from the terminal.

Removal of such data is absolutely necessary for PCI DSS compliance. The PayEx Nordic Paymentapplication performs secure deletion of CHD and SAD, and the customer has no responsibilities in this matter.

On very rare occasions, for debugging purposes, it may be necessary to collect encrypted SAD orCHD prior to authorization. In such cases, the terminal must be returned to PayEx for forensics. PayEx follows these principles:
- Collect sensitive authentication only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete such data immediately after use.

If merchant systems contain CHD in any form, even if encrypted, such data must be securely deletedafter expiration of customer defined retention period. Simply deleting the files is not sufficient

NIST-800-88r1 publication (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 88r1.pdf) contains information on how to perform secure deletion of sensitive data on various me-dia.

As CHD and SAD are stored internally in the terminal prior to authorization, the customer has noresponsibilities for securely deleting such data after any retention period. The PayEx application handles this.

Likewise, the terminal always stores PANs in an unreadable format, and performs secure deletion ofencrypted CHD after authorization. The customer therefore has no responsibilities for ensuring that PANs are rendered unreadable. The PayEx application handles this.

5.2. Do not use production data in the PayEx Test Environment.

When developing new integrations, ECR Integrators typically work with test terminals, in a test environment. These terminals can be identified by the string "Special Mockup" blinking inred, so that the terminal cannot be used in production. These terminals are configured to use the PayEx Test Environment. Integrators are not allowed to use production cards in such terminals. PayEx can provide a suite of test cards for use with these terminals.

5.3. Masked PAN for business needs

PAN is never displayed in the full form.
Cardholder receipts will only provide the last four digits of the PAN in clear.
Merchant receipts will only provide the first six and last four digits of the PAN in clear. Logfiles contains only truncated PAN showing only first six and last four digits of the PAN.
Customer/Resellers/Integrators are not allowed to see the full PAN or to change PAN display set-tings.

If Customer/Resellers/Integrators for some reason could access the PAN in clear form, they are ad-vised that is their direct responsibility to render the PAN unreadable in all such instances using strong cryptography and secure deletion methods.
PAN must always be rendered unreadable or secured with strong cryptography whenever it is sentvia end-user messaging technologies, like e-mail, chat, etc..
NIST Special Publication 800-57, Part 1, Rev. 4 contains information on encryption methods andusage (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf).

5.4. Protection of keys and cryptographic materials

Merchants and integrators cannot and do not manage encryption keys. The terminal's encryption keys are embedded in the terminal and cannot be retrieved. A terminal that reaches its End of Lifemust be returned to PayEx.

Data encryption keys are injected by PayEx using hardware, software and procedures provided bythe terminal manufacturer within a key injection facility. PayEx operators can't access to the unen-crypted key because everything is managed by the hardware vendor service and infrastructure.

Encryption keys are stored in tamper evident/resistant areas of the terminal. Any attempt, from amalicious individual, to retrieve keys from the device, either physically or logically, will result inthe destruction of those encryption keys.

Customers and integrators/resellers do not have access to the

encryption keys.Key-management process is in charge to the

hardware vendor.

Application does not store cryptographic key material.

If the terminal's tamper detectors are triggered, either by accident(shaking the terminal violently, bad power supplies, irregular temperature changes, etc) or by attackers attempting to compromise
the device, it will immediately become useless. The message "ALERT IRRUPTION" will blink. Insuch cases, the terminal should be returned to PayEx. If you have an idea of what happened, pleaseinclude a brief description with the terminal.

The merchant should always keep in mind that the terminal processes money and its cryptographickeys are sensitive. If merchants and other operators, for any reason, suspect that someone have at-tempted to compromise the device or the environment it operates in, they should contact PayEx support, who will advise further. If they suspect that someone attempted to compromise the deviceitself, a support ticket should be opened and the device should be returned for forensics.

5.5. Secure authentication

Application does not provide or use or manage any authentication credentials or default account.Moreover, application does not provide any default account with administrative access.

Customer/Resellers/Integrators are advised about that all access to PCs, servers, and databases withpayment applications or cardholder data must require a unique user ID and a PCI DSS compliant secure authentication.

5.6. Application level logging

Logging is enabled by default, as required by PA-DSS section 4. Disabling logs would result intonon-compliance with PCI DSS. All changes to the terminal configuration is logged by the PayExterminal management systems.

Customer/Resellers/Integrators are not allowed to change log configuration. Only authorized vendorpersonnel can change the software configuration.

The following events are logged by default:

- All individual access to the application (via the terminal keyboard, as no non-console admin-istrative access is provided by the application/OS/hardware).
- All actions taken by any individual;
- Invalid logical access attempts;
- Use of identification and authentication mechanisms
- Initialization of the audit logs;
- Creation and deletion of system-level objects is not possible through the payment applica-tion.

Each logged event contains:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
  - Identity or name of affected data, system component, or resource

Failure to maintain these logs will result in non compliance with PCI DSS

All logs are locally stored in the terminal and can be transmitted to the terminal management systemcentral logging service. Events are stored in a central database and are available to the customer through the terminal management system interface. It is possible to configure the terminal manage- ment system to send online logs to an external storage. Refer to the Terminal Management System user manual for details.

If for any reasons, as for troubleshooting purpose, some logs, containing PAN or SAD, were col- lected by the customer, in compliance with the PCI-DSS requirements following recommendationslisted below must be followed:

- Secure elimination of collected sensitive data after the resolution of problems.
- Collected data must be gathered only to solve a specific problem.
- These data should be stored only in specific locations with limited access.
- Collect only the limited amount of data necessary to solve a specific problem.
- The sensitive data must be encrypted at the time of storage.
- These data must be disposed of safely immediately after use.

5.7. Software Version Methodology

Following the SDLC and the PA-DSS Program Guide, software version methodology follows thisschema: A.B.C

Version numbers consists of three digits separated by a dot: A.B.C.

Numbers reflect the change impact descriptions of the as per the PA DSS program guide:

- “A” number changes when High Impact Changes happens to the software;
- “B” number changes when Low Impact Changes happens to the software;
- “C” number is used as wildcard and changes when a corrective modification is issued (i.e., bug fixing) or of anomaly corrections that DO NOT have an impact on security or any otherPA-DSS requisite.

Please refer to the PA-DSS Program Guide for further details,
available athttps://www.pcisecuritystandards.org/document_library

5.8. Wireless networking

The payment application itself does not require wireless technology, nor are wireless applicationsbundled with the payment application.

Wi-fi enabled terminals must always be only accessible through the merchant’s own, securednetwork, and the network must be secured in a PCI DSS compliant way

Furthermore, for payment applications using wireless technology, payment application must facili-tate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption forauthentication and transmission.

Note 1: The use of WEP as a security control is prohibited.

Some general rules shall be applied when using wireless technology:

- Encryption keys were changed from default at installation, and are changed anytime anyonewith knowledge of the keys leaves the company or changes positions.
- Default SNMP community strings on wireless devices were changed.
- Default passwords/passphrases on access points were changed.
- Firmware on wireless devices is updated to support strong encryption for authentication andtransmission over wireless networks (for example, WPA2).
- Other security-related wireless vendor defaults, if applicable.
- Install perimeter firewalls between any wireless networks and the cardholder data environ- ment, and configure these firewalls to deny or control (if such access is required for businesspurposes) any traffic from the wireless environment into the cardholder data environment.
- Ensure wireless networks transmitting cardholder data, or connected to the cardholder dataenvironment, use industry best practices (for example, IEEE 802.11i) to implement strongencryption for authentication and transmission.

We strongly encourage our customers to refer to the PCI SSC wireless guidelines when implementing such technologies:

https://www.pcisecuritystandards.org/documents/pci_dss_wireless_guideline_info_sup.pdf

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Wireless_Guidelines.pdf

5.9. Hardware and software dependencies

5.9.1. Ingenico OS requirements

PayEx is responsible for installing and upgrading the Ingenico OS on the terminals. The customer,reseller or integrator has no responsibilities in this regard.

5.9.2. Standalone terminals

Standalone terminals have no software dependencies. They only require a network connection(seethe Network Implementation section).

5.9.3. ECR terminals(iPPs and unattended terminals)

ECR-enabled terminals require an ECR component running on the ECR device(for instance a Win-dows PC). The terminal can use either a TLV-based or a JSON-based ECR protocol. ECR integra- tors receive the protocol documentation for both protocols as part of their training materials. For new integrators, PayEx recommends using the JSON-based protocol. PayEx also provides a mid- dleware solution “PosPay” which runs on the ECR. The PayEx terminal application supports Po- sPay version 4.16.x or newer.

5.9.4. mPOS terminals(iSMPs)

mPOS-terminals are mobile terminals with mobile ECRs running on Android, iOS, or mobile Win- dows devices. These require an Ingenico component on the ECR device.This add on is provided by PayEx to the integrators. mPOS terminals use the PayEx JSON interface, and have some support forthe PayEx TLV interface. Only the JSON interface will be supported in the future.

Ingenico Add on	Recommended addon version	OS version supported by Ingenico
Add on PCL for Windows	2.13.00	Windows 7: 32-bits and 64-bits Windows 8, 8.1: 32-bits and 64-bits Windows XP SP3 32-bits (only USB connec-tivity is supported) Windows 10: 32-bits and 64-bits (No USB driver automatically installed on Windows 10)
Add on PCL for iOS	2.23.00	iOS 8.1.0 or newer. See the add on documen- tation for any known issues on iOS versions.
Add on PCL for Android	1.13.00	The Android devices must run under OS ver-sion 2.3.4 or higher to use the Bluetooth con-nectivity. To use the USB connectivity, OS version mustbe 3.1 or higher. See the add on documentation for any knownissues with Android versions or specific de- vices.

5.10. Network Implementation

Payment application and underlying operating system uses and enables only required services, pro-tocols and ports.

Outgoing Connection	Transmitted data	Protocol	Ports
Transactions for non-iSMP termi-nals.	MACed transactions with encrypted SAD(pinblock) and CHD(track 2, PAN).	TLS 1.1 or newer	9034
Transactions for iSMP terminals.	MACed transactions with encrypted SAD(pinblock) and CHD(track 2, PAN).	TLS 1.1 or newer	443
PayEx-TMS	Terminal logs, terminal configuration files.	TLS 1.1 or newer	9045,443
Ingenico-TMS	OS and application upgrades, terminal configuration files	TLS 1.1 or newer	7003, 7005, 7007

Possible communication channels with the ECR are:

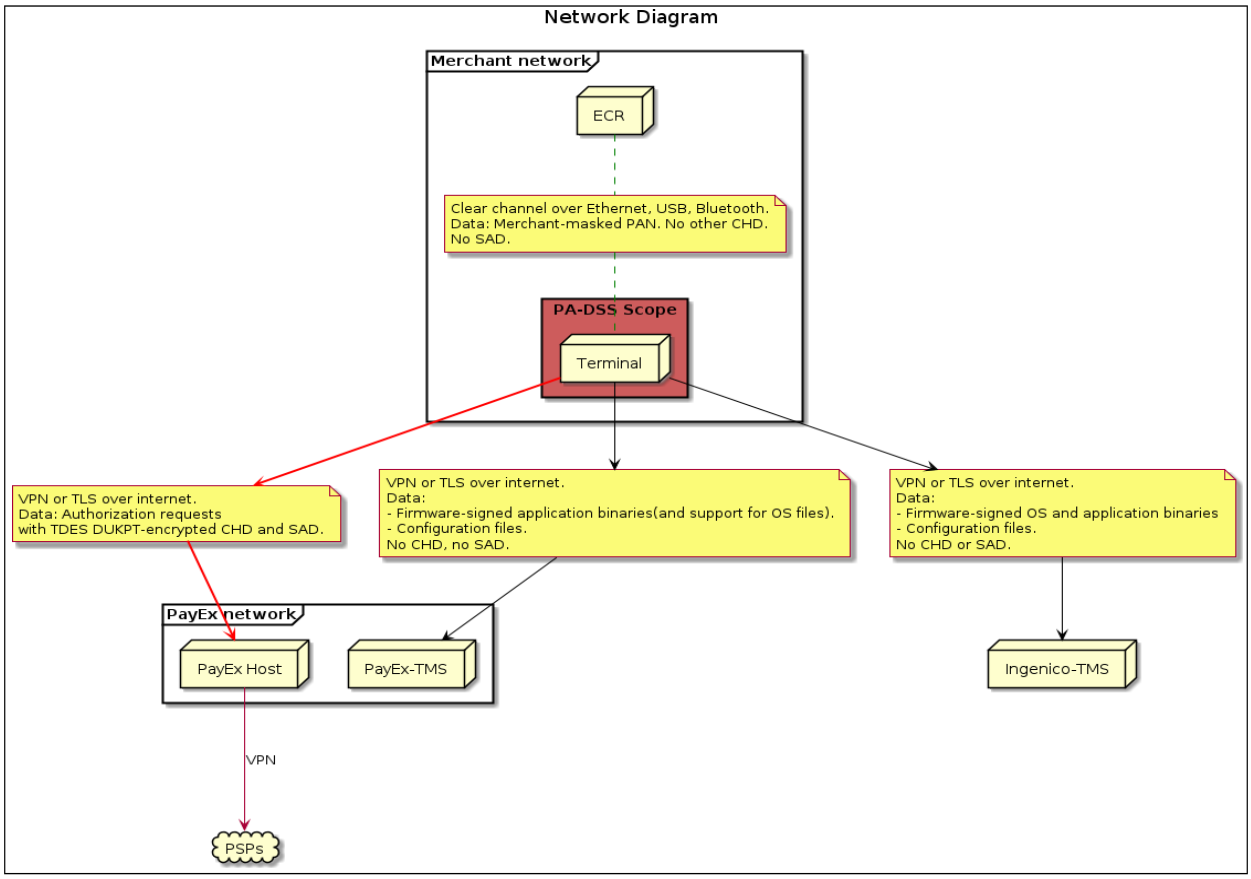
Endpoint	Channel	Protocol	Transmitted data	Ports
ECR	USB	TCP over PPP	Transaction data without CHD or SAD	5188
ECR	Ethernet	TCP	Transaction data without CHD or SAD	5188
ECR	Bluetooth	TCP	Transaction data without CHD or SAD	9599

Do not store CHD, even if encrypted, on Internet-accessible systems, like DMZ systems. Payment application does not store CHD in clear form in any circumstance.
Application does not provide any kind of remote access to the operating system or to the customer environment by the software vendor nor to Integrators and resellers. Payment application does not facilitate non-console administrative access.

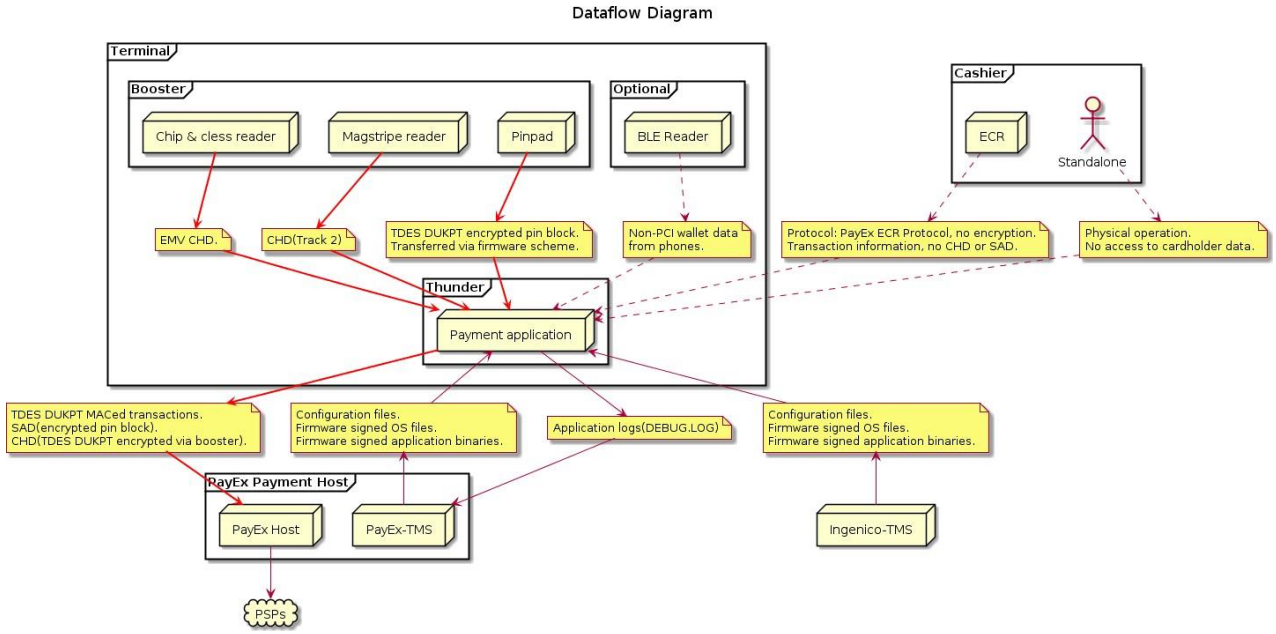
Payment application does not use any end-user messaging technologies (for example, e mail, instantmessaging and chat) for sending CHD.

CHD and SAD is never sent through end-user messaging technology.

Here is a example of a common network implementation, in which bold red arrows means sensibledata in communication:



A data flow diagram follows, in which bold arrows mean sensitive data in communication:



Remote updates

There is no automatic update process that identifies and downloads available payment applicationupdates.

Payment application upgrades are performed on demand using the Terminal Management System(TMS).

Payment application is configured to check for software updates daily. The application connects to the TMS host and checks if updates are available.

If updates are available, they are downloaded and automatically installed.

Any application binaries are verified and validated directly by the underlying operating system usingvendor signing system. Application binaries are digitally signed by PayEx using certified hardware from thehardware vendor and if a signature mismatch happens the binaries are discarded and not installed.

An e-mail will be sent to all customers and resellers as soon as a new package will be available. At the same time will be commuanicated how software will be securely deployed.

5.11. Secure data transmission

The application uses TLS 1.2 in data transmissions over public channels. In certain cases, TLS 1.1 may be used. TLS 1.0 is never used.

Resellers, integrators and customers are advised that if they use any other application to send PANs with end-user messaging technologies; they must use a solution that implements strong cryptog- raphy.

5.12. Storage of cardholder data on a server connected to the internet

PA-DSS requirement 9.1 states that compliant payment applications must be developed so that cardholder data are not stored on the same server as public(internet)-facing servers. As terminals, like all offline capable terminal payment applications, stores encrypted cardholder data prior to authorization, they must not be directly exposed to the internet e.g placed on a DMZ.

Payment terminal IP and ports for merchants using SLL / TLS

Endpoint	Address:Port
Authorization host	postx.payex.com:443
Authorization host	postxdirect.payex.com:443
Ingenico TMS	91.208.214.34:7005
Ingenico TMS	91.208.214.34:7007
PayEx-TMS	postms.payex.com: 443

Payment terminal IP and ports for merchants using MPLS or IPSec VPN

Endpoint	Address:Port
Authorization host	postx.payex.com:9010-9050
Ingenico TMS	Ingestate.payex.com:9048
PayEx-TMS	postms.payex.com: 9045

Middleware solution “PosPay”

Endpoint	Address:Port
Authorization host	posconfiguration.payex.com:443

PayEx handles all configuration of the terminals, the merchant’s only responsibility is to configure the network access.”