PA-DSS IMPLEMENTATION GUIDE

Nets Oy

Merchant Solutions

Ingenico Telium Terminals

Terminal Software T21

Version 2.3

DOCUMENT DETAILS

Author:	**Arto Kangas**
Date:	**06.02.2015**
Version:	**1.8**

Version information

Date	Change log	Version	Author
1.11.2011	Draft	0.1	AKa
1.6.2012	First release	1.0	AKa
24.8.2012	Added list of PCI PTS approved hardware	1.1	AKa
6.9.2012	Instructions for PC access control	1.1	AKa
11.1.2013	Annual review. No changes.	1.1	AKa
18.6.2014	Changed used IP addresses and ports to connect to the host	1.2	AKa
23.6.2014	Review for new terminal software version 2.2.x	1.2	AKa
26.6.2014	Added name T21 for terminal software. Changed all Luottokunta company name to Nets. Added information how integrators are informed about IG.	1.3	AKa
26.6.2014	Recommendation to setup Wi-fi security. Added info to remove all possible sensitive data from old setup.	1.4	AKa
10.7.2014	Added information about displaying PAN	1.5	SKa
23.7.2014	Adding versioning details and adjusting requirements related to centralized logging and audit trails.	1.6	HKo
27.10.2014	Changed referenced PA-DSS version to 3.0. Added rows to table in chapter 3.5 (customer responsibilities).	1.7	AKa
06.02.2015	Review for new terminal software T21 version 2.3.	1.8	AKa
01.04.2015	Added definition for about document version to header and T21 SW version 2.3 to front page (to avoid misunderstanding).	1.8	AKa

Contents

1. INTRODUCTION

1.1. Intended audience

- Payment terminal and application integrators, merchants or their representatives
- Implementation guide can be used e.g.
    - By customers installing or integrating the payment solution
    - During training sessions related to the payment terminal and application

2. IMPLEMENTATION GUIDE

2.1. Introduction to PA-DSS

This is the Implementation Guide (IG) document meeting the requirements from PA-DSS (Payment Application - Data Security Standard) version 3.0 Appendix A. The intent of the Implementation Guide is to guide merchants, integrators and their representatives for securely deploying or implementing the payment application.

PA-DSS requirements are available from PCI SSC (Payment Card Industry Security Standards Council) website https://www.pcisecuritystandards.org/. The PA-DSS applies to software vendors and others who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement. Standard applies to payment applications that are sold, distributed, or licensed to third parties.

The payment application for the payment terminals is developed according to the PA-DSS requirements. The payment application is responsible for processing the cardholder data.

In case of the POS integrated solutions; the sales application running POS terminal (cash register) is not subject to PA-DSS requirements. The sales application running on POS terminal does not have access to cardholder data.

Merchants, other customers, resellers and integrators are responsible for installing or deploying the payment application according to software vendor instructions. The goal is securely installing, deploying or configuring the PA-DSS compliant payment application into a PCI DSS compliant environment.

2.2. Implementation guide review and updates

Implementation guide is reviewed at least annually and when new minor or major versions of the payment application are released. Implementation guide is updated as a result of the review if needed.

2.3. Dissemination of the Implementation guide

Implementation guide is available to all relevant payment application users (including customers or integrators). Dissemination is done after any updates to implementation guide. Latest version of the implementation guide is available through Nets web site: http://www.netskauppa.fi/tl/Extranet/.

Every time new or existing integrator starts using or updates version to PA-DSS validated software, Nets customer and integrator support departments will inform them to read through PA-DSS Implementation Guide.

2.4. Payment application information

The following chapter identifies the payment application for which this Implementation Guide was written for.

Payment application	Details
Name	T21
Version	2.2.x
Dependencies	Ingenico Telium terminals: EFT930G (GPRS) EFT930S (LAN) EFT930B (Bluetooth) iCT250 (LAN) iWL250G (3G) iWL250B (Bluetooth) iPP350 (Integrated) ML30 (Integrated)

The payment application is developed for Ingenico's PCI PTS approved payment card terminals. PCI-PED and PCI-PTS approvals are listed in annex A.

2.4.1. Version Numbering

The used version methodology is X.Y.Z that described the level of changes related to PA-DSS requirements.

X – This is the major change version (revision) number. It is always planned. When this is incremented the release could involve major compatibility issues with previous releases. The first number is used to indicate the major changes of the software release. This is a fundamental change in the way an application functions and will alter the security of the application or how cardholder data flows through the application. This will require a full assessment including testing the change against all PA-DSS requirements and submitting a new Report on Validation (ROV). Examples of these types of changes are:

- Changes that directly impact components of the application which performs the authorization or settlement of the payment transaction, such as any change that can be tied to a PA-DSS requirement.
- Changes that impact the approved underlying operating system or platform.
- Changes made to how cardholder data is stored, processed or transmitted such as adding a new authentication module or database.

Y – This is the minor change version number. It can be planned or unplanned and changes regularly. When this is incremented the release could involve minor compatibility issues with previous releases. This is a change to the non-core functionality of the application and changes the look and feel of the application without impacting its security or the cardholder data flow. This will not require a full assessment but a Minor change attestation will be completed and submitted to update the version number listed on PCI SSC's website. For example version 1.0.0 would be updated to version 1.1.0. Examples of these types of changes are:

- Changes that impact the aesthetics of the payment application, such as GUI enhancements, button movement, marketing color updates, etc.
- Changes that impact components of the application that are not related to the authorization or settlement process of the payment application, such as adding additional tax fields not related to cardholder data, updates to the Implementation Guide, etc.
- Changes to the type, formatting and presentation of reports, for example changing the size or font, adding additional non cardholder data field

Z – This is the release (service pack) number. It is typically unplanned and changes frequently as fixes are issued. When this is incremented the release will not involve any compatibility issues with previous releases. This digit is the only wildcard component of version number and it would represent an internal non-compliance and non-security related change. The change doesn't impact directly an application in PA-DSS scope. Use of release (service pack) number for any change that has an impact on application security or any PA-DSS Requirements is prohibited.

The version number indicates the release version number and it is not bind directly to any software module version number.

3. CUSTOMER RESPONSIBILITIES

Application is solely running on Ingenico's PCI PTS approved payment card terminals. Nets is responsible for installing and configuring the application on the terminal. Due to the nature of the application, the customer responsibilities are very limited.

3.1. Access control and passwords

The PCI DSS requires that access to all systems in the payment processing environment to be protected through the use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of generic group accounts used by more than one user or process. Additionally any default accounts provided with operating systems, databases and/or devices should be removed/disabled/renamed, or at least should have PCI DSS compliant complex passwords and such accounts should not be used.

Examples of default administrator accounts include e.g. “administrator” (Windows systems), “sa” (SQL databases) and “root” (UNIX/Linux).

The payment application does not provide access to cardholder data nor does it provide administrative access. There are no authentication and authorization mechanisms.

3.2. Cleaning cardholder data

If the merchant has stored cardholder data before implementing this PA-DSS approved application, merchant is responsible for the clean-up procedures of their legacy environment.

The previous versions of this payment application have not stored cardholder data in customer environment.

3.3. Network configuration

It is recommended that there are no direct connections from Internet or other public networks to the payment terminal. Usage of firewall, masquerade (hide) NAT or other traffic filtering is not mandatory.

The payment application requires the following outbound network connectivity.

- TCP/8892) to varma1.manison.fi, varma2.manison.fi and varma3.manison.fi
- UDP/53 for DNS resolving

In addition, the payment application requires DNS resolving (udp/53) to operate properly.

The payment application does not require inbound network connections except the incoming packages from already established connections.

3.4. Wireless communication configuration

Bluetooth models with base (iWL250B and EFT930B): The pairing is done with dedicated infrared or contact interface. The transmission is secured by the payment applications confidentiality and integrity controls. T21 terminals do not directly use Wi-Fi network.

In case Wi-Fi is used to connect integrated terminals to network the wireless implementation has to be done in secure manner. Refer to requirements 6.2 and 6.3 under chapter 3.5.

3.5. Requirements and customer responsibilities

The following table presents the merchant, other customer, reseller or integrator responsibilities in installing, deploying and/or using the payment application.

Req	PA-DSS topic	Customer responsibilities
1.1.4	Delete sensitive authentication data stored by previous payment application versions.	There are no customer responsibilities. The payment application does not store sensitive authentication data. Terminals are prepared and applications are installed by Nets.
1.1.5	Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.	There are no customer responsibilities. Requirement is not applicable for the payment application. The payment application does not store sensitive authentication data. Sensitive authentication data is not gathered as part troubleshooting or debugging the payment application.
2.1	Purge cardholder data after customer-defined retention period.	There are no additional customer responsibilities due to the payment application. Merchant needs to meet PCI DSS requirements in their business. Merchant does not have access to cardholder data via the payment terminal or application. Cardholder data is not printed or otherwise stored within the merchant environment. Cardholder data is rendered by the application (strong encryption, truncation and hashing in use). Merchant does not have access to clear-text data. In addition, in Nets solution the merchant does not have access to rendered cardholder data and merchant never has access to decryption keys. *Note! If a merchant has stored cardholder data before implementing this PA-DSS approved application, merchant is responsible for the clean-up of their legacy environment.*
2.2	Mask PAN when displayed so only personnel with a business need can see the full PAN.	There are no additional customer responsibilities due to the payment application. Merchant needs to meet PCI DSS requirements in their business. PAN is masked on all printed receipts and is only displayed on POS terminal display in full when card details are entered manually.

Req	PA-DSS topic	Customer responsibilities
2.3	Render PAN unreadable anywhere it is stored.	There are no customer responsibilities. PAN is rendered unreadable by the application and stored within PCI PTS approved payment terminal. The payment application does not provide access to cardholder data.
2.4	Protect keys used to secure cardholder data against disclosure and misuse.	There are no customer responsibilities. PKI technology is used for encryption. The payment application includes a public key for encrypting the data. The public key is a part of the application binary protected by integrity controls (signed binary). The corresponding private key is stored only in the backend systems. Customers or payment application has no access to the private key.
2.5	Implement key management processes and procedures for cryptographic keys used for encryption of cardholder data.	There are no customer responsibilities. Customer is not responsible for key management. Key management processes and procedures are not part of the payment application. Nets does key management in the backend systems, key management procedures meet the PCI DSS requirements.
2.5.1 – 2.5.7	Implement secure key-management functions	There are no customer responsibilities. Customer is not responsible for the key management. Key management processes and procedures are not part of the payment application. Nets does key management in the backend systems, key management procedures meet the PCI DSS requirements.

Req	PA-DSS topic	Customer responsibilities
2.6	Render irretrievable cryptographic key material or cryptograms stored by previous payment application versions.	There are no customer responsibilities. Customer is not responsible for key management. Previous versions of the payment application by Nets have not stored cryptographic key materials or cryptograms in customer environment. Note! If the merchant has stored cardholder data, cryptographic key materials or cryptograms before implementing this PA-DSS approved application, merchant is responsible for the clean-up procedures of their legacy environment. Clean-up procedure needs to meet the industry best practices for secure deletion.
3.1	Use unique user IDs and secure authentication for administrative access and access to cardholder data.	Requirement is not applicable for this payment application. There are no customer responsibilities. The payment application does not provide access to cardholder data nor does it provide administrative access. There are no authentication and authorization mechanisms.
3.2	Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	Requirement is not applicable for this payment application. There are no customer responsibilities. The payment application does not provide access to cardholder data nor does it provide administrative access. There are no authentication and authorization mechanisms.
4.1	Implement automated audit trails.	There are no customer responsibilities. The payment application does not provide access to cardholder data nor does it provide administrative access. The file integrity monitoring events are logged to TMS host and customers may be provided with logs upon request.
4.4	Facilitate centralized logging.	There are no customer responsibilities. The payment application does not provide access to cardholder data nor does it provide administrative access. The file integrity monitoring events are logged to TMS host and customers may be provided with logs upon request.

Req	PA-DSS topic	Customer responsibilities
5.4.4	Implement and communicate application versioning methodology	Version methodology is described in chapter 2.4.1. Customer should verify that the version they are using meets the PA-DSS requirements and is valid for deployments.
6.1	Securely implement wireless technology.	Bluetooth models with base (iWL250B and EFT930B): The pairing is done with infrared or contact interface. The transmission is secured by the payment applications confidentiality and integrity controls. Bluetooth models without base (iWL250B): The pairing is done with the rules and procedures described in chapter 3.3. The transmission is secured by the payment applications confidentiality and integrity controls. Note! The payment application secures the transmission and cardholder data by encrypting the cardholder data and with integrity controls. Cardholder data can only be decrypted in the Nets backend systems. In addition, there are integrity controls for communication to prevent tampering the messages.

Req	PA-DSS topic	Customer responsibilities
6.2, 6.3	Secure transmissions of cardholder data over wireless networks.	The payment application secures the transmission and cardholder data by encrypting the cardholder data and with integrity controls. Cardholder data can only be decrypted in the Nets backend systems. In addition, there are integrity controls for communication to prevent tampering the messages. However, if wireless networks are used in customer's environment, customer is responsible for: - Changing all wireless default encryption keys, passwords and SNMP community strings upon installation; - Changing wireless encryption keys, passwords and SNMP strings anytime anyone with knowledge of the keys/passwords leaves the company or changes positions; - Install a firewall between any wireless networks and systems that store or process cardholder data, and to configure firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment; - Using industry best practices (for example, IEEE 802.11.i) to provide strong encryption for authentication and transmission.

Req	PA-DSS topic	Customer responsibilities
8.2	Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.	There are no customer responsibilities regarding configuration of the payment application and it's services. The payment application only runs in PCI PTS approved payment terminal. The application can not be installed on cash registers, POS terminals, workstations or servers. Integrated payment terminal models require USB communication with the POS terminal. It is recommended that there are no direct connections from Internet or other public networks to the payment terminal. The payment application does not require inbound network connections except the incoming packages from already established connections.
9.1	Store cardholder data only on servers not connected to the Internet.	Requirement is not applicable for this payment application. There are no customer responsibilities. The payment application is running on PCI PTS approved payment terminal.
10.1	Implement two-factor authentication for remote access to payment application.	Requirement is not applicable for this payment application. There are no customer responsibilities. The payment application does not provide remote access.
10.2.1	Securely deliver remote payment application updates.	Requirement is not applicable for this payment application. There are no customer responsibilities. The payment application updates are not delivered via remote access. The payment application uses "call home" functionality for checking and receiving updates. The integrity of the updates is verified.
10.2.3	Securely implement remote access software.	Requirement is not applicable for this payment application. There are no customer responsibilities. The payment application does not provide remote access.

Req	PA-DSS topic	Customer responsibilities
11.1	Secure transmissions of cardholder data over public networks.	There are no customer responsibilities. The payment application secures the transmission and cardholder data by encrypting the cardholder data and with integrity controls. Cardholder data can only be decrypted in the Nets backend systems. In addition, there are integrity controls for communication to prevent tampering the messages.
11.2	Encrypt cardholder data sent over end-user messaging technologies.	Requirement is not applicable for this payment application. There are no customer responsibilities. The payment application does not use or support usage of end-user messaging technologies.
12.1, 12.2	Encrypt non-console administrative access.	Requirement is not applicable for this payment application. There are no customer responsibilities. The payment application does not provide non-console administrative access.

4. SECURING CARDHOLDER DATA

4.1. Key management

The key management is done by Nets. The key management meets the PCI DSS requirements. There are no customer responsibilities regarding key management.

The key management and encryption depends on PKI (public key infrastructure). Encryption is done with public key cryptography. The payment application has access only to the public key. The corresponding private key is only available in the Nets backend system. The integrity of the public key is controlled by application signing procedures.

Customer or payment application does not have access to the decryption (private) keys.

4.2. PAN

PAN information is displayed in the following instances:

- Customer's receipt (masked PAN)
  - On receipt printed by the terminal
  - On receipt data sent to Lumo
- Merchant's receipt (masked PAN)
  - On receipt printed by the terminal
  - On receipt data sent to Lumo
- T21 screen when authorization by phone is required (full PAN)

By default, the payment application masks the PAN on all displays. There is one exception, where the full PAN is shown: If authorization by phone is initiated, the full PAN is shown on T21 screen. Phone authorization is used when authorization is required, but network connections are temporarily down. Apart from the phone authorization, there is no other legitimate business need for users to see the full PAN.

5. GLOSSARY

PCI - Payment Card Industry
PCI SSC – Payment Card Industry Security Standards Council
PA-DSS – Payment Application Data Security Standard
PCI DSS – Payment Card Industry Data Security Standard
PCI-PTS – Payment Card Industry PIN Transaction Security
PA-QSA – Payment Application Qualified Security Assessor

References

Payment Card Industry Data Security Standard (PCI-DSS)

Payment Application Data Security Standard (PA-DSS)

ANNEX A: PCI PTS APPROVALS

IPP3xx **Hardware #:** IPP3xx-11Txxxxx **Firmware #:** 820305V02.xx, 820365V02.xx, 820528v02.xx **Applic #:** 820073v01.xx	4-20184	3.x	PED 30 Apr 2020
iCT2xx **Hardware #:** iCT2xx-11Txxxxx **Firmware #:** 820305V02.xx, 820365V02.xx, 820528v02.xx **Applic #:** 820073v01.xx	4-20196	3.x	PED 30 Apr 2020
IWL2xx **Hardware #:** IWL2xx-11Txxxxx **Firmware #:** 820518V01.xx, 820365V02.xx, 820528v02.xx (SRED) **Applic #:** 820073v01.xx	4-20179	3.x	PED 30 Apr 2020
IWL2xx **Hardware #:** IWL2xx-01Txxxxx **Firmware #:** 820305V01.xx, 820365V02.xx, 820528v02.xx (SRED) **Applic #:** 820073v01.xx	4-20181	3.x	PED 30 Apr 2020
ML30 **Hardware #:** ML30-xxxx-0101 **Firmware #:** 820065V01.03 **Applic #:** V03.xx	4-20035	1.x	PED 30 Apr 2014
EFT930 **Hardware #:** EFT930x-xxxx0101, EFT930B-xxxx0201, EFT930x-xxxx1101, EFT930x-xxxx2101, EFT930X-XXXX3101, EFT930x-xxxx0102, EFT930x-xxxx1102, EFT930x-xxxx2102, EFT930x-xxxx3102, EFT930x-xxxx0103 **Firmware #:** V01.01, 820065V01.03 **Applic #:** V03.xx	4-20012	1.x	PED 30 Apr 2014

METATIEDOT

Nro	Metatietoluokka	Metatieto
1.00	**YLEISTIEDOT**	
1.01	Tuottaja	Sisäinen
1.03	Omistajarooli	Product Manager
1.04	Omistajan nimi	Arto Kangas
1.05	Varaomistajarooli	Johtaja, Maksupääteliiketoiminta
1.06	Varaomistajan nimi	Jukka Sippola
1.07	Masterversion nimi	PA-DSS Implementation Guide
1.08	Dokumentin nimi	PA-DSS Implementation Guide
1.12	Kieli	Englanti
1.13	Masterkieli	Englanti
1.14	Ylädokumentti	
1.15	Kuvaus	PA-DSS Implementation Guide
1.16	Version kommentti	
1.17	Avainsanat	PA-DSS, Implementation Guide
2.00	**EHEYS**	
2.01	Muokkausajankohta	11.1.2013
2.02	Muokkaaja	Arto Kangas
2.03	Laatija	Arto Kangas
2.04	Katselmoitava	Kyllä
2.05	Katselmoijien roolit	Tuotepäällikkö, Tuotetuki, ICT Kehitys, Liiketoimintajohtaja
2.06	Katselmoijien nimet	Arto Kangas, Juha Korhonen, Jussi Paasonen, Jukka Sippola
2.07	Hyväksyjien nimet	Jukka Sippola
2.11	Luontiajankohta	9.10.2012
2.12	Hyväksymisajankohta	11.1.2013
2.16	Katselmointiväli	1 vuosi
	Päivitysmuistutus	15.10.2013
2.17	Vanhenemisajankohta	11.1.2014
2.18	Tila	Hyväksytty
2.19	Versio	1.1
	DOKUMENTIN TYYPPI	
3.03	Dokumenttityyppi	Ohje
3.04	Dokumenttityypin alatyyppi	Käsikirja
	TURVALUOKKA	
4.01	Turvaluokitus	Luottamuksellinen
	SENSITIIVISTÄ TIETOA SISÄLTÄVÄT	
5.01	Korttinumeroita (PAN)	Ei
5.02	PCI DSS alaista tunnistustietoa	Ei
5.03	Henkilötietoja	Ei
5.04	Pankkisalaisuuden alaista asiakastietoa	Ei
5.05	Liikesalaisuuksia	Ei
5.06	Varautumiskriittistä aineistoa	Ei

Nro	Metatietoluokka	Metatieto
	KÄYTETTÄVYYS	
6.01	Kohderyhmän ylätaso	Nets+kumppanit
6.02	Kohderyhmän alataso	
6.03	Kohderyhmä roolitaso	
	ARKISTOINTI	
8.01	Sähköisen dokumentin tallennuspaikka	P:\Projektit\PA-DSS Maksupääte\05. Audit materials
8.03	Säilytysaika	Toistaiseksi
8.05	Säilytysajan peruste	Liiketoimintaperuste
9.00	**TEHTÄVÄRYHMÄ**	
9.01	Tehtävä	
9.05	Järjestelmä/sovellus	Maksupääte