NixPAY version 02.00.XX Implementation Guide with Atos Worldline terminals

Nixor EE AS

April 1, 2020

Revision History

Revision	Date	Author(s)	Description
1.0	08.04.14	T. Drenkhan	Created initial draft
1.1	26.04.14	T. Talvik	Added acquirers connection parameters and initial setup information
1.2	26.09.14	T. Talvik	Added Swed LV, LT connection parameters
1.3	24.10.14	T. Drenkhan	Updated to fit PA-DSS requirements
1.4	04.11.14	T. Drenkhan	Updated secure remote connection creating information
1.5	11.11.14	T. Drenkhan	Added change history, key management update
1.6	29.11.14	T. Drenkhen	Added detailed description of key management
1.7	24.04.15	T. Drenkhen	Rephrased versioning scheme, added pre-authorization file locations
1.8	19.11.15	T. Drenkhen	Documented TLS usage instead of SSL
1.9	14.01.16	T. Drenkhen	Added instructions to follow industry best practices
1.10	26.01.16	T. Drenkhen	Added payment application version and dependencies. Clarified IG providing instructions.
1.11	03.02.16	T. Drenkhen	Added additional Dependencies. Clarified cardholder data storage, sending and deletion. Changed application version to use wildcards.
1.12	10.03.16	T. Talvik	Changed solution name from "NixPay PA-DSS" to "NixPAY".
1.13	08.12.16	T. Drenkhan	Updateted to match NixPAY version 01.01.XX, improved logging section
1.14	11.04.17	T. Drenkhan	Clarified according to PA-DSS v3.2
1.15	10.04.18	T. Drenkhan	Updated application version to 01.02.XX
1.16	20.09.18	T. Drenkhan	Fixed application version on page 5
1.17	26.09.18	T. Drenkhan	Added terminal inspection instructions
1.18	16.05.19	T. Drenkhan	Rephrased key managment in section 2.5
1.19	07.06.19	T. Drenkhan	Updated TLS version in use
1.20	12.09.19	T. Drenkhan	Updated to match NixPAY version 01.03.XX
1.21	01.10.19	T. Drenkhan	Improved transactional info locations for SAMOA 2 and SPICA, added NixManager info
1.22	03.10.19	T. Drenkhan	Defined keyloading and bookkeeping ports. Clarified key storage on SAMOA 2 and SPICA terminals
1.23	30.01.20	T. Drenkhan	Added referece to external versioning documentation

1.24	27.02.20	T. Drenkhan	PA version 02.00.xx, added terminals hardware and PTS certificates to dependency list, updated IG download reference

Contents

Nomenclature

NixEFT **Application running in the terminal which handles payment cards and carries out EMV transaction by communicating with the Acquirer.**

NixLoader **Application software manager. Connects to managment server and performs required actions. For example downloads application updates and manages SSL certificates.**

NixPay **Whole system including NixEFT, NixLoader, terminal hardware and other applications related to payment application, such as ECR integration specific components.**

1 Introduction

The purpose of this document is to describe implementing **NixPAY** version **02.00.XX** to the merchant system under Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS) requirements, which will support a merchant's Payment Card Industry Data Security Standard (PCI DSS) compiliance efforts. More information about PCI DSS and PA-DSS can be found at `https://www.pcisecuritystandards.org`.

2 Document usage

For each PA-DSS requirement there is a short description and explanation how it is resolved in NixEFT application, which is the payment application of NixPAY solution. Also there are additional steps for merchant and/or System Installer to ensure system compliance with PCI DSS. Both the System Installer and the controlling merchant must read this document. This document must also be used when training ECR integrators/resellers at initial workshops.

3 Dependencies

NixPAY depends on **stunnel**, which is used to secure communication between acquirer and payment application with TLS encryption.

The application is meant to run only on **Worldline terminals** (Valina, Yomani XR/ML, Yomani XR/ML Touch, Yomova Countertop, Yomova Portable and Yoximo) which are running on SAMOA 2 or SPICAplatform.

To fulfill centralized logging requirement **log4net** is used in ECRs. There is also TMS in use to faciliate the requirement.

Terminal hardware and certificates dependencies

Manufacturer	Model	PTS Approval
Atos Worldline	Yomani ML/XR	4-30092 (3.x) 4-30194 (4.x)
	Yoximo	4-30094 (3.x) 4-30213 (4.x)
	Yomova	4-30136 (3.x) 4-30203 (4.x)
	Valina	4-30222 (4.x)

4 Requirement 1: Do not retain full track data, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data

Requirement 1.1.1: Do not store full track data after to the authorization.

NixPAY compliance with requirements

NixPAY does not store full track data after the authorization is completed.

Your actions

No additional actions are required.

Requirement 1.1.2: Do not store card verification value or code after to the authorization.

NixPAY compliance with requirements

NixPAY does not store card verification value or code after the authorization is completed.

Your actions

No additional actions are required.

Requirement 1.1.3: Do not store PIN or PIN block after to the authorization.

NixPAY compliance with requirements

NixPAY does not store PIN or PIN block after the authorization is completed.

Your actions

No additional actions are required.

Requirement 1.1.4: Delete sensitive authentication data stored by previous payment application versions.

NixPAY compliance with requirements

NixPAY does not store sensitive authentication data nor has it stored in earlier versions. This means that there is no need for historical data removal.

Your actions Make sure to remove all sensitive data (full magnetic-stripe data, CVV2 and cardholder data) from other devices (ECRs, PCs, servers, etc.) used in Your systems. Please refer to corresponding vendor user manual. Historical data removal is necessary for PCI DSS compliance.

Requirement 1.1.5 Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.

NixPAY compliance with requirements

NixPAY does not store sensitive authentication data for troubleshooting purposes.

Your actions

- 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.

5 Requirement 2: Protect stored cardholder data

Requirement 2.1: Securely delete cardholder data after customer-defined retention period.

NixPAY compliance with requirements

No cardholder data except PAN and expiration date are stored in the PTS-approved terminal. This storage is encrypted to meet the PCI DSS requirements. Cardholder data is securely deleted after successful transactions capture (batching) process or in case of pre-authorization after reversal or completion. Capture process is automatically started once per day at Acquirer-defined time.

List of locations where cardholder data is stored in the different terminal types.

In SAMOA 2 family terminals the transactional data is kept in following files:


```
/root/NixEFT/transactions/{acquirer_id}/xxxxxx.dat,
/root/NixEFT/transactions/{acquirer_id}/xxxxxx.rec,
/root/NixEFT/transations/{acquirer_id}/preauth/xxxxxx.dat,
/root/NixEFT/transations/{acquirer_id}/preauth/xxxxxx.rec,
/root/out/bk/{acquirer_id}/xxxxxx.csv,
/root/out/ra/{acquirer_id}/xxxxxx.csv
```

While using SPICA family terminals the transactional data is sandboxed into the payment application directory `/data/data/ee.nixor.spica.nixeft/files`:

```
./usr/transactions/{acquirer_id}/xxxxxx.dat,
./usr/transactions/{acquirer_id}/xxxxxx.rec,
./usr/transations/{acquirer_id}/preauth/xxxxxx.dat,
./usr/transations/{acquirer_id}/preauth/xxxxxx.rec,
./out/bk/{acquirer_id}/xxxxxx.csv,
./out/ra/{acquirer_id}/xxxxxx.csv
```

where x is number from 0 to 9 and {acquirer_id} is unique identifier for each acquirer activated in terminal.

Additional places depending on the integration:

Receipts are sent to the Cash register PC for printing.

Your actions

In case of integrated system do not store the receipts electronically in the ECR system. In case storing is required electronic receipts must be encrypted with strong cryptographic and securely removed, following NIST or other approved standard for secure data removing,when receipts are not required anymore.

In case of standalone version additional actions are not required.

It is possible to manually start the capture process to delete cardholder data stored in the PTS-approved terminal, if needed. Storage, sending and deleting of cardholder data are automated and cannot be configured by the application user.

Requirement 2.2: Mask PAN when displayed so only personnel with a business need can see the full PAN.

NixPAY compliance with requirements

PAN is always masked expect on offline transaction merchant receipt as required by the Acquirer and on the terminal screen for voice authorization in order to facilitate a single transaction. Remark at PCI DSS Requirement 8 says that access to one card number at a time does not require unique ID for tracking activity.

Your actions

Protect from unauthorized access all media including receipts with unmasked cardholder data as mandated by PCI DSS requirement 9.

Requirement 2.3: Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs).

NixPAY compliance with requirements

PAN is stored in two encrypted files in PED. On offline merchant receipt, full PAN is shown as required by the Acquirer; this is in accordance with PCI DSS requirement 3.3. On all other receipts and terminal screens pan is masked so, that only last 4 characters are shown.

Your actions

Additional actions are not required.

Requirement 2.4: Protect keys used to secure cardholder data against disclosure and misuse.

NixPAY compliance with requirements

All keys related to customer data storing are located in secure tamper proof memory unit (MP1 for SAMOA 2, PA for SPICA) and managed by the terminal itself.

Your actions

Additional actions are not required.

Requirement 2.5: Implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data.

NixPAY compliance with requirements

At the moment all keys used in Worldline terminals are loaded by the manufacturer to the tamper proof memory unit associated with MP1 for SAMOA 2 terminals or PA for SPICA termials. This is done by PCI rules. Keys for data encryption which are created at the first bootup of the terminal (scheme currently in use) or loaded to the MP1/PA during the personalization process (done by Worldline, currently not used). The rotation period for data encryption keys is a maximum of 1 year for each file, then a new key is generated and the data is re-encrypted. Each file is crypted with a different random derivate of the master key, (e.g. file1 is cryped using driversifier 93, and file2 is cryped with driversifier 86).

Manufacturer key for Swedbank is loaded to the terminal during the personalization process - each terminal receives its own unique key derivation. This manufacturer key is shared between Worldline and Swedbank. Following is general description how keys which are used for data operations will be loaded to terminals.

From terminal key derivation data is extracted and provided to the Swedbank security center where they can regenerate the derivated key from manufacturer key. This derivated key is used to encrypt new terminal keys which are

then sent to terminal using secure communication channel. In case of terminal receives and successfully loads new keys the whole key chain will be under control of Swedbank - manufacturer key is replaced by Swedbank key. Just described process does not affect other keys for other acquirers.

Your actions

In case of cryptographic key compromise is detected or suspected it must be immediately reported to the system vendor.

Requirement 2.6: Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.

NixPAY compliance with requirements

The key management process is automatic and controlled only by the NixEFT application running inside the terminal. It does not require any key injections from outside. A 3DES key is used for encryption. The key is generated and stored in the Point of sale Tamper resistant module (POS TRM) and never leaves the terminal.

- The 3DES encryption key is generated by the terminal's operating system.
- The encryption key is stored in tamper evident memory by the terminal's operating system.
- Key transmission is not required.

Your actions

Additional actions are not required.

6 Requirement 3: Provide secure authentication features

Requirement 3.1: Use unique user IDs and secure authentication for administrative access and access to cardholder data.

NixPAY compliance with requirements

No administrative access to terminal is allowed and there are no application accounts possible to create. Cardholder data stored in the terminal cannot be accesed outside the terminal.

Your actions

Additional actions are not required.

Requirement 3.2: Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.

NixPAY compliance with requirements

Nixor does not provide any accounts to access payment application and sensitive data related to it.

Your actions

Additional actions are not required.

Requirement 3.3: Secure all payment application passwords during transmission and storage.

NixPAY compliance with requirement

There are no passwords stored or transmitted to/from the terminal.

Your actions

Additional actions are not required.

Requirement 3.4: Payment application must limit access to required functions/resources and enforce least privilege for built-in accounts

NixPAY compliance with requirement

There are no built-in accounts used in NixPAY payment application.

Your actions

Additional actions are not required.

7 Requirement 4: Log payment application activity

Requirement 4.1: Implement automated audit trails.

NixPAY compliance with requirements

There are no configurable logging options in the NixPAY application, logging is automatically enabled and can't be disabled or configured by the application user. There is no user access to cardholder data within or by the application, there are no user accounts in the application. All events related to PA DSS requirements are automatically enabled to be logged, which is limited to the creation and deletion of system level objects.

Your actions

Additional actions are not required.

Requirement 4.2: Payment application must provide automated audit trails.

NixPAY compliance with requirements

There is no access to the cardholder data within the payment application.

Your Actions

Additional actions are not required.

Requirement 4.3: Audit trail entries event logging.

NixPAY compliance with requirements

There are no user login allowed to the application.

4.3.1 User identification - there is no user login and therefore no need for user identification.

4.3.2 Type of event - The type of event is in log as freeform text.

4.3.3 Date and time - Timestamp is in the beggining of each log line.

4.3.4 Success or failure indication - The process result is logged. There are 5 different levels used for logging:

- DEBUG - Designates fine-grained informational events that are most useful to debug an application.
- INFO - Designates informational messages that highlight the progress of the application at coarse-grained level.
- WARNING - Designates potentially harmful situations.
- ERROR - Designates error events that might still allow the application to continue running.
- FATAL - Designates very severe error events that will presumably lead the application to abort.

4.3.5 Origination of event - There are keywords used to determine the source of the event:

- BK - Actions specific to bookkeeping.
- RA - Actions specific to receipt archive.
- TL - Actions which are involved with terminal software update.
- NFC - Actions related to contactless kernel.
- EMV - Actions related to contact kernel.
- [0xXXXXXXXX] - Actions related to loyalty services to handle loyalty cards, where X is a HEX digit from 0 to F.

- <no keyword> - Actions specific to current state of the application. Application logs state changes.

4.3.6 Identity or name of affected data, system component, or resource - Creation and deletion of transaction base in terminal are logged. Also Creation and deletion of bookkeeping files. (See 5 for list of files that are created and removed.)

Log example of system level objects deletion:

```
2016-02-03 00:18:05,733 [6] DEBUG PEDLog - Application entered Periodic state
2016-02-03 00:18:08,738 [6] DEBUG PEDLog - Removing /root/NixEFT/transactions/000007.dat
2016-02-03 00:18:10,530 [6] DEBUG PEDLog - [BK] removed /root/out/bk/000009.csv
2016-02-03 09:47:09,404 [6] DEBUG PEDLog - [RA] removed /root/out/ra/000076.csv
```

Your Actions

Additional actions are not required.

Requirement 4.4: Facilitate centralized logging.

NixPAY compliance with requirements

Fixed amount of logs are kept in terminal and all logs are sent to ECR where logs are handled by log4net module. It is possible to configure log4net module to implement centralized logging to merchant provided arbitrary server.

In addition it is possible to collect logs via central terminal managment system Xenturion. However these logs are uploaded on demand or on reaching threshold limit i.e. not uploaded as they are generated.

Your actions

If You like to set up an arbitrary server to collect logs please refer to log4net manuals at `http://logging.apache.org/log4net/` for further details. Disabling or preventing logging will result in non-compppliance with PCI DSS and PA DSS.

8 Requirement 5: Develop secure payment applications

Requirement 5.4.4: Implement and communicate application versioning methodology.

NixPAY compliance with requirements

The application versioning has three majority ranks (xx.yy.zz). The first section presents if there has been major changes in the application. The second section indicates smaller changes, but influential to application. The third section is wildcard which indicates bugfixes and very minor changes in application behaviour.

Major change version number(xx). The major change release is always planned and can include modifications which influence compatibility issues. It also may involve changes in security implementation or cardholder dataflow. Major release requires full PA-DSS ROV assessment. Examples:

- Changes that that can be directly 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.

Minor change version number (yy). The minor changes are also planned. Minor changes are related with GUI, translations, receipts and other functionalities which are not tied to the PA-DSS requirements. These modifications do not require full PA-DSS ROV assessment to be conducted, but a Minor change attestation will be completed and submitted. Examples:

- Additional language support addition
- Changes in menu colors, button layout, screen pictures, screen/receipt fonts
- Changes in receipt formation
- Additional acquirer communication specification implementation

No/low impact change (wildcard) version number (zz). These changes are mainly unplanned and are required to establish/maintain normal application workflow. These changes represent non-security and non-compatibility related changes.

Your actions

Additional actions are not required.

Requirement 5.4.5 Internal and external versioning documentation.

NixPAY compliance with requirements

Please see “Version mapping.doc”.

Your actions

Additional actions are not required.

9 Requirement 6: Protect wireless transmissions

Requirement 6.1: Securely implement wireless technology.

NixPAY compliance with requirements

NixEFT application can work in network behind firewall and in network without a firewall. There are supported strong encryption for wireless technology: WPA and WPA2. All data sent to and from NixEFT application is encrypted with TLS1.2 or higher except communication between ECR and NixEFT, and for logging. Connections which do not use TLS do not include any sensitive data and can be conducted over serial or wireless communication.

Your actions

It is required that merchant, if using wireless communication, has installed firewalls which deny or control any traffic (if such traffic is necessary for business purpose) from the wireless environment into NixPAY application environment. Additional information can be found from Your firewall manual.

In case wireless network is used, make sure that following requirements are met (use industry best practices (for example, IEEE 802.11.i)):

- Default wireless encryption keys, passwords and SNMP community strings are changed at installation.
- Wireless encryption keys, passwords and SNMP community strings must be changed if anyone with knowledge of the keys/passwords leaves the company or changes positions.
- Wireless encryption keys, passwords and SNMP community strings must be changed if any wireless components provided with, but not controlled by, the payment application is added.
- Firmware on wireless devices must be updated to support strong encryption, WPA/WPA2. Please note that the use of WEP as a security control was prohibited as of 30 June 2010.

Payment application uses total of 4 different ports. More detailed description can be found in the Table 1.

Table 1: Outgoing ports used by applications running in the terminal

Port	Purpose	Includes sensitive data	Uses TLS
5434	Communication with the ECR	No, except PAN and expiration date on offline receipt[1]	No
9876	System management service	No	No
8080[2]	Communication with additional bookkeeping server. Data uploaded to the server includes, but is not limited to payment receipts with truncated PAN (first six and last 4 digits only) and batch reports. [3]	No	Conditional[4]
Periodic[5]	Periodic data exchange with the Acquirer: • Transactions capture, • EMV public keys update, • Acquirer parameters update, • Stoplist update	Yes	Yes
Auth.[5]	Transaction authorization with the Acquirer	Yes	Yes
Keyloading[5]	Acquirer key managment (e.g. online PIN)	No	Yes

Requirement 6.2: Secure transmissions of cardholder data over wireless networks.

NixPAY compliance with requirements

NixEFT supports strong wireless encryption WPA and WPA2. All data sent to and from payment application is protected with TLS1.2 or higher encryption

[1] Merchant can ask the Acquirer to set the floor limit to 0 which forces all transactions to be authorized online. This means that PAN and expiration date will always be masked on the receipt.

[2] This is default port which can be changed according to the particular installation. There could also be several ports in use for customer specific solutions.

[3] Exchanged data depends on particular solution and additional client application loaded to the terminal. Please see specific application documentation for exact ports.

[4] TLS is not enforced, could be enabled for particular installation

[5] Exact port is Acquirer dependent, please see Appendix B for further details

excepted communication between ECR and application, and logs transmission. Communications not using TLS do not contain cardholder sensitive data.

Your actions

Additional actions are not required.

Requirement 6.3: Provide instructions for secure use of wireless technology.

See Requirement 6.1 described above.

10 Requirement 7: Test payment applications to address vulnerabilities and maintain payment application updates

Requirement 7.2.3: Provide instructions for customers about secure installation of patches and updates.

NixPAY compliance with requirement

Merchants are informed before update by e-mail or other agreed communication method within sufficient time.

For updating centralized server is used where terminal asks updates from.

All packages and updates are digitally signed. This signature is checked in terminal with hash validation - if package has been tampered with the signature is rejected and update is not installed to the terminal. This ensures files integrity and that only validated software is installed to the terminals.

Your actions

Additional actions are not required.

11 Requirement 8: Facilitate secure network implementation

Requirement 8.2: Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.

NixPAY compliance with requirements

There are no services like file-sharing, FTP, NetBIOS running on the terminal. For communication over public network TLS encryption is used. On the ECR PC runs NixEFT Service, which acts as intermediary between ECR software and NixEFT payment application running on the terminal. This service listens for connections from both parties.

Your actions

Additional actions are not required.

12 Requirement 9: Cardholder data must never be stored on a server connected to the Internet

Requirement 9.1: Store cardholder data only on servers not connected to the Internet.

NixPAY compliance with requirements

NixPAY does not store cardholder data on servers connected to the Internet.

Your actions

In case integration with ECR is used storing the offline transaction receipts to the public facing systems are prohibited. However if the storage is needed no Internet access to the ECR is allowed and strong cryptography must be used..

Otherwise if it is not public facing system or integration with ECR then additional actions are not required.

13 Requirement 10: Facilitate secure remote access to payment application

Requirement 10.1: Implement multi-factor authentication for all remote access to payment application that originates from outside the customer environment.

NixPAY compliance with requirements

No remote access is allowed to payment application.

Your actions

If remote access is implemented into the environment, the following secure configurations must be considered:

- In addition to username and password other factors must be implemented, such as, but not limited to:
  - Personal certificates
  - OTP token
  - Smart card
- Use only secure protocols for remote access such as TLS, SSH, IPSEC or encrypted VPN
- Do not use default passwords for remote access

- Configure the firewall to only allow trusted sources for remote connections
- Implement and enforce strong access controls and passwords according to industry accepted standards, at a minimum according to PCI DSS requirement 8.x.
- Do not allow 3rd party access by vendors and resellers unless absolutely necessary and only allow such connections under a limited period of time.

Requirement 10.2.1: Securely deliver remote payment application updates.

NixPAY compliance with requirements

Terminal with payment application cannot be accessed remotely. All signed updates are downloaded from Nixor terminal management system (Xenturion), i.e. there is no need to deliver updates to customers on removable media. Customers are communicated with before update process is started.

Your actions

If remote access is implemented into the environment, the following secure configurations must be considered:

- In addition to username and password and 2nd factor must be implemented, such as, but not limited to:
  - Personal certificates
  - OTP token
  - Smart card
- Use only secure protocols for remote access such as TLS, SSH, IPSEC or encrypted VPN
- Do not use default passwords for remote access
- Configure the ECR firewall or dedicated firewall for the ECR environment to only allow trusted sources for remote connections
- Implement and enforce strong access controls and passwords according to industry accepted standards, at a minimum according to PCI DSS requirement 8.x.
- Do not allow 3rd party access by vendors and resellers unless absolutely necessary and only allow such connections under a limited period of time.

Requirement 10.2.3: Securely implement remote-access software.

NixPAY compliance with requirements

No remote access is allowed to the payment application.

Your actions

If remote access is implemented into the environment, the following secure configurations must be considered:

- Change default settings in the remote-access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins. More info in Section E.
- Use only secure protocols for data exchange such as TLS, SSH, IPSEC or encrypted VPN.
- Enable account lockout after a certain number of failed login attempts. More info in Section E.
- Establish a VPN connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer environments to authorized personnel.

14 Requirement 11: Encrypt sensitive traffic over public networks

Requirement 11.1: Secure transmissions of cardholder data over public networks.

NixPAY compliance with requirements

All cardholder data sent from the NixEFT application is protected with TLS1.2 or higher.

Your actions

In case of integration if the receipts are forwarded they must be encrypted with strong cryptographic and only trusted keys/certificates may be accepted. Otherwise additional actions are not required.

Requirement 11.2: Encrypt cardholder data sent over end-user messaging technologies.

NixPAY compliance with requirements

NixPAY does not use any end-user messaging technologies.

Your actions

In case of integration if the receipts are forwarded they must be encrypted with strong cryptographic. Otherwise additional actions are not required.

15 Requirement 12: Secure all non-console administrative access

Requirement 12.1: Encrypt non-console administrative access.

NixPAY compliance with requirements

Terminal cannot be accessed remotely and no non-console access is possible.

Your actions

In case of integrated system remote access to the ECR is used, it must be non-console and secured as described in Requirement 10 and use strong cryptography. Otherwise no additional actions are required.

Requirement 12.1.1: Encrypt non-console administrative access.

While using secure connection make sure key length is corresponding to latest requirements, minimum public key length is 2048 since 1st of January 2014. Also clear-text protocols such as Telnet or rlogin must never be used for administrative access.

- More information about SSH can be found at `http://www.openssh.com/`.
- More information about VPN can be found at `http://www.openvpn.net/`.
- More information about TLS can be found at `https://www.openssl.org/`.

Requirement 12.2: Use multi-factor authentication for all personel with non-console administrative access.

In case non-console administrative access is granted to CDE (Cardholder Data Environment) multi-factor authentication must be implemented and used.

16 Requirement 13: Maintain a PA-DSS Implementation Guide for customers, resellers, and integrators

16.1 Requirement 13.1: Develop, maintain, and disseminate a PA- DSS Implementation Guide(s) for customers, resellers, and integrators

The PA-DSS Implementation Guide is disseminated to all customers, resellers, and integrators whenever new version of application is released/installed. In case customers, resellers, and integrators request the PA-DSS Implementation Guide it can be re-sent.The newest version of Implementation Guide is available on

Nixor's webpage (https://www.nixor.ee/jaekaubandus/makselahendus/kaardimakse/) where it can be downloaded.

17 Regular terminals inspection

It is required to regulary inspect terminals by the merchant and report to terminal provider if tampering is detected (e.g. added card skimmers, unauthorized terminal substitution etc). Terminal swapping/reaplacing must be agreed with the terminal provider and logged atleast with the following details: date and time, terminal replacement reason, name and signature of the person performing the swap.

In case merchant has replacement terminals on the site these must be protected from unauthorized access. This also includes terminals awaiting for repair or maintenance.

A Installing the system

Installing Atos Worldline terminal drivers

It is necessary to install Atos drivers for terminals which are communicating with ECR over serial port. Installing drivers for Windows XP, Vista, 7: run driver installation script or executable according to operating system.

To install POS to Windows 8/10 it is required to disable driver signature verification for installation procedure. Search for „Advanced start-up options“ and select "Restart now", then select "Troubleshoot" -> "Advanced options" -> "Start-up Settings" -> "Restart". Before starting to load OS new prompt screen will be displayed, select option with "Disable driver signature enforcement" and install drivers as described in previous section.

Setting up Internet Connection Sharing for the terminal

Run script "setup_terminal_network.cmd" as administrator or setup network manually: Open "Network Connections" Open PC main internet connection properties and select "Sharing". Enable ICS (Allow other network users to connect ...) and click OK. In case there are more than 1 connection select the connection with "Atos Worldline" in description. Configure Atos connection ipv4 to ip: 192.168.137.1, subnet: 255.255.255.0, if possible.

B TCP ports used by different Acquirers

Table 2 lists TCP ports parameters used by different Acquirers. This information is useful for properly configuring Firewalls and monitoring network activity.

Acquirer	IP	Authorization	Periodic	Keyloading
Swedbank EE	193.203.197.216	9997	9996	9990
Swedbank LV	193.203.197.216	7502	7501	9990
Swedbank LT	193.203.197.216	9999	9998	9990
Nets EE	194.204.43.40	8042	8043	-

Table 2: Supported Acquirers and their connection parameters.

C Terminal management TCP ports

The terminals software is updated and managed remotely using ports 5012 and 5014. Terminals monitoring is conducted using the same ports (certificate expiration alerts, remote configuration, etc). This information is useful for properly configuring Firewalls and monitoring network activity.

D TLS configuration using NixLoader/NixManager

NixLoader/NixManager only allows to select between predefined acquirers which are added to the terminal by installing the definition package. In addition to acquirer selection it is required add certificate to the terminal to use for establish connection. It is not possible to add random certificate, but only certificate which request is generated from private key located in terminal. More information about certification request generation and request signing can be found from "SSL connection between the Nixor's NixPAY payment solution and the Acquirer's payment host".

E Setting up secure authentication

- Configure any administrative accounts for all necessary software and change all default passwords.
- Each user must have his/her own user account.
- At least one of following authentication methods must be used:
  - Password or passphrase
  - Token device
  - Smart card
  - Biometrical identification
- No group, shared or generic accounts and passwords may be used.
- All passwords must have a minimum length of seven characters and contain both numeric and alphabetic characters.
- The password is required to be changed at least every 90 days.

- New password must not match any of the last four passwords used.
- No more than 6 repeated unsuccessful logon attempts are allowed by locking the user account.
- The user lockout is a minimum of 30 minutes or until an administrator enables the user ID.
- If the session has been idle more than 15 minutes re-authentication is required.

F Secure key-management

Cryptographic key distribution is done by Nixor using HSM and special protocol. The distributed cryptographic keys are stored in tamper-proof memory in terminal MP1. All key exchanging and management is done by Nixor.

Secure key generation

Use only secure key types for example AES or DES3 keys. For key generation secure Random Bit Generator (e.g. HSM functionality) or coin flipping should be used. The coin must be flipped as many times as there are bits in the key (e.g. AES 128 -bit key requires 128 flips). Each flip result is marked as corresponding key bit. For security reasons keys should be composed in 2 to 6 parts which are XOR-ed together in HSM or other secure module

G PA-DSS requirements index

PA-DSS Requirement	PA-DSS Topic	Page
1.1.1	After authorization, do not store the full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	7
1.1.2	After authorization, do not store the card verification value or code (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	7
1.1.3	After authorization, do not store the personal identification number (PIN) or the encrypted PIN block.	7
1.1.4	Delete sensitive authentication data stored by previous payment application versions.	8
1.1.5	Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.	8
2.1	Securely delete cardholder data after customer-defined retention period.	8
2.2	Mask PAN when displayed so only personnel with a business need can see the full PAN.	9
2.3	Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs).	10
2.4	Protect keys used to secure cardholder data against disclosure and misuse.	10
2.5	Implement key- management processes and procedures for cryptographic keys used for encryption of cardholder data.	10
2.5.1-2.5.7	Implement secure key- management functions.	25
2.6	Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.	11
3.1	Use unique user IDs and secure authentication for administrative access and access to cardholder data.	11
3.2	Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	12

PA-DSS Requirement	PA-DSS Topic	Page
3.3	Secure all payment application passwords during transmission and storage.	12
3.4	Payment application must limit access to required functions/resources and enforce least privilege for built-in accounts.	12
4.1	Implement automated audit trails.	12
4.2	Payment application must provide automated audit trails.	13
4.3	Audit trail entries event logging.	13
4.4	Facilitate centralized logging.	14
5.4.4	Implement and communicate application versioning methodology.	14
5.4.5	Internal and external versioning documentation.	15
6.1	Securely implement wireless technology.	16
6.2	Secure transmissions of cardholder data over wireless networks.	17
6.3	Provide instructions for secure use of wireless technology.	18
7.2.3	Provide instructions for customers about secure installation of patch es and update s.	18
8.2	Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.	18
9.1	Store cardholder data only on servers not connected to the Internet.	19
10.1	Implement multi-factor authentication for all remote access to payment application that originates from outside the customer environment.	19
10.2.1	Securely deliver remote payment application updates.	20
10.2.3	Securely implement remote-access software.	20
11.1	Secure transmissions of cardholder data over public networks.	21
11.2	Encrypt cardholder data sent over end- user messaging technologies.	21
12.1	Encrypt non-console administrative access.	22
12.1.1	Encrypt non-console administrative access.	22
12.2	Use multi-factor authentication for all personel with non-console administrative access.	22
13.1	Develop, maintain, and disseminate a PA-DSS Implementation Guide(s) for customers, resellers, and integrators	22