Poplatek PCI PA DSS Implementation Guide

Payment Card Core 2.2.x

Table of Contents

1 Version history

Version	Date	Author	Description
1.4	2015-07-29	DFo	**PA DSS v3.1** related updates: - Explicit troubleshooting guidance - Retention policy clarified for merchants - Explicitly TLS 1.2 - Clarified centralized logging 5.6 - Updated Appendix A - Clarified distribution of this document - Updated 5.5 Key Management - Removed SW library versions - Clarify IG distribution process
1.4.1	2016-01-27	DFo	- X.Y.pp and subtitle for the document
1.4.2	2016-04-05	DFo	- Editorial
2.0	2017-06-29	JRä	- Describe how masked PANs are generated - Remove text that does not require customer actions - Rename CardSvc to Payment Card Core - Add Spire and Spica update descriptions - Add Payment Frontend description - Fix Payment Card Core version to 2.0.x - Remove section Cardholder data handling as unnecessary - Clarifications related to requirements 2.1, 2.2, 11.1, 11.2 - Include versioning character set and clarify version numbering component descriptions - Terminology correction Poplatek PA → Payment Card Core
2.0.1	2018-06-11	JRä	- Update company: Poplatek Oy → Poplatek Payments Oy
2.2	2018-10-26	JRä	- Update Payment Card Core version - Update PAN masking description to match Payment Card Core 2.2.x

2 Introduction

The Payment Card Industry Data Security Standard (PCI DSS) [1] specifies requirements for the configuration, operation and security of payment cards transactions. These requirements apply to organizations that store, process or transmit cardholder information and target to prevent credit card fraud and to increase security.

The requirements for the Payment Application Data Security Standard (PA DSS) [2] are derived from the PCI DSS Requirements and Security Assessment Procedures. The PA DSS applies to software vendors and others who develop payment applications (PA) that store, process, or transmit cardholder data as part of authorization or settlement, where these payment applications are sold, distributed, or licensed to third parties.

The purpose of this PA DSS Implementation Guide is to instruct Merchants, Resellers and Integrators on how to implement Payment Card Core into their environment in a PCI and PA DSS compliant manner. It is not intended to be a complete installation guide. Integrators may include e.g. Electronic Cash Register (ECR) vendors integrating Poplatek payment terminal with their POS system using Poplatek POS protocol [3], or Vending Machine vendors integrating Poplatek payment terminal into the vending machine.

> **NOTE**: Merchant/Reseller/Integrator responsibilities and actions are are marked with **Merchant actions** in this document.

Version and review history is shown in 1. This section 2 provides introduction, describes the review and update process, lists abbreviations and references. Payment application usage is described in section 3 and the PA details are described in section 5 including centralized logging. Troubleshooting information is provided in section 6. Appendix A in section 7 lists and addresses all the PA DSS requirements related to this document.

2.1 Review and update process

Poplatek must review this document on an annual basis and update it as needed to document all major and minor changes to the payment application Payment Card Core module.

The PA DSS scope is the Payment Card Core module only. Changes outside the Payment Card Core module need not to described or managed with the PA DSS Implementation Guide review process. If this scope is changed by PA DSS QSA, this document must be updated to reflect the new scope. Also, this document is updated and reviewed in a timely manner whenever the PA DSS standard is updated.

Review process includes Poplatek internal review by an individual other than the editor of the change knowledgeable of the Payment Card Core module internals. Document must be reviewed by a PA DSS QSA, during the minor and major change control process with the QSA.

2.2 Distribution

This document is initially distributed to all customers, resellers, and integrators latest with the first product delivery via customer service portal. Each of will be notified when this document is updated along with the updated document

This update notification happens through the customer service portal. This portal lists the IG version number and a link to this document. Whenever this document is updated, approved, and applicable to the payment terminals on the field with customers, the IG is uploaded to the *Poplaview* service portal and the link to the document is updated.

Note also that the latest version of this guide can be obtained by sending email to support@poplatek.fi. The master document is stored into the Poplatek internal version management system.

2.3 Abbreviations

CHD	CardHolder Data
ECR	Electronic Cash Register
PA	Payment Application
PAN	Primary Account Number
PA DSS	Payment Application Data Security Standard
PCI DSS	Payment Card Industry Data Security Standard
POS	Point-of-Sale
QSA	Qualified Security Auditor
TLS	Transport Layer Security

2.4 References

[1] Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures Version 3.1, April 2015, PCI Security Council.

[2] Payment Card Industry (PCI) Payment Application Data Security Standard, Requirements and Security Assessment Procedures Version 3.1, May 2015, PCI Security Council.

[3] Poplatek POS Protocol Version 0.8, November 2013, Poplatek.

[4] Information Supplement Skimming Prevention: Best Practices for Merchants, Version 2.0, September 2014, PCI Security Council

3 Payment Application usage

Strong access control measures must be used in all PCI scoped system components by using unique user Ids, strong passwords, and PCI DSS compliant secure access authentication, for more details see [1]. However, note that when using Poplatek Payment terminal there is no need to handle or store cardholder data outside the terminal.

In the Payment Card Core there are no user configurable settings in the payment terminal. Also, there are no user accounts (or administrative accounts) to be configured or any user passwords/credentials to be updated or reset.

Poplatek apayment terminal supports POS integration with Poplatek POS protocol. Poplatek payments terminal can only be used with Poplatek payment gateway.

Poplatek payment terminalrequires Internet connection for communicating with the payment gateway. Either USB or Ethernet wiring can be used to provide the network connection and connection with the POS. USB wiring requires Atos USB drivers, which provide Ethernet-over-USB and USB-serial. The USB serial is not used, only the Ethernet-over-USB or Ethernet if it is connected. 3G, Wireless LAN or IP traffic tunneled through Bluetooth RFCOMM may be used for commuincation if wireless commication is preferred.

4 Installation environment

4.1 Payment Terminal handling

The payment terminal must be installed according to Poplatek installation instructions and along the Merchant actions requirements described in this document. Payment terminals must be periodically inspected for evidence of tampering and substitution (e.g. additions of card skimming devices) and merchant personnel must be trained for payment terminal inspections (see [4]). Also, an up-to-date list of payment terminals must be kept either by Merchant or provided by Poplatek.

- **Merchant actions**: Train personnel working with payment terminals on how to inspect payment terminals for evidence of tampering and substitution. The training must include at least the following:
  - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot payment terminals.
  - Do not install, replace, or return payment terminals without verification.
  - Be aware of suspicious behavior around payment terminals (for example, attempts by unknown persons to unplug or open devices).
  - Report suspicious behavior and indications of payment terminal tampering or substitution to appropriate personnel (for example, to a manager or security officer).
- **Merchant actions**: Inspect payment terminals for evidence of tampering and substitution periodically. The period can be based on Merchant's own risk analysis (e.g. whether the terminals are unattended or attended, in public environments or in stores).
- **Merchant actions**: Merchant must have payment terminal registry for all its payment terminals. For Poplatek payment terminals, this registry can be provided by Poplatek. If provided by Poplatek, ensure Poplatek has most up-to-date information about each payment terminal. The registry must include model of the device, location, and device serial number. Merchant must inform Poplatek, whenever a payment terminal is relocated, decomissioned, removed, or added into production.

Network firewall configurations

There are no specific requirement on network segmentation when using Poplatek apayments terminal and when the Poplatek payments terminal is the only medium used to read payment cards. See above.

- **Merchant actions**: Poplatek payment terminal uses external service provided only by Poplatek. For the Poplatek apayment terminal the TCP port *443* for host *pt.api.poplatek.com and port 443 for host atos-update.prod.poplatek.fi* to the Internet (outbound) must be opened. Also DNS resolution for the host must be allowed. In addition port *10001* must be allowed to connect to the payment terminal (inbound) from the ECR (when integrated with ECR). See protocols below.

4.2 Wireless LAN

If merchant uses wireless LAN to route the Poplatek payment terminal connection to the Internet or the payment terminal uses wireless technology, it must be configured securely. This means that PCI DSS requirements must be followed when implementing the wireless networks:

- **Merchant actions**:
    - Encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves the company or changes positions.
    - Default SNMP community strings on wireless devices must be changed.
    - Default passwords on access points must be changed.
    - Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks. WEP algorithm is not allowed.
    - Any security-related wireless vendor defaults must be changed, if applicable.
    - The default Service Set ID (SSID) must be changed. Also, the SSID must not be broadcasted.
    - Firewall(s) must be installed between any wireless networks and systems that store cardholder data. This firewall(s) must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment.

5 Payment Application

5.1 Initial Payment Card Core distribution

The Payment Card Core is initially distributed along with the payment terminal or if absent, the payment terminal will install the Payment Card Core from the update server during first boot with network connection. In any case, during the boot up sequence the Payment Card Core will be updated from the update server if needed.

5.2 Versioning scheme for Payment Card Core module

The versioning scheme for the Payment Card Core module is **XX.YY.pp** where the components are as follows:

XX This is the major version number (numeric values 01-99) and would represent a security impacting change in the Payment Card Core module, e.g. adding considerable new features to the card number handling and management.

YY This is the minor version number (numeric values 00-99) and would represent a minor enhancement to the Payment Card Core module. Minor change could change source code related to cardholder sensitive data handling, but do not impact security critical functionality.

pp The patch level (numeric values 00-99) is wildcard (*). Patch level changes never include security or PA DSS requirement impacting changes. Patch level changes are for example editorial changes like comment updates.

Change in versioning components XX and YY require PCI PA-DSS verification.

5.3 Required components and protocols

5.3.1 Hardware dependencies

Poplatek PA uses hardware provided by the Atos Worldline or Spire Payments payment terminal manufacturers.

Dependent Atos Wordline hardware are:

Atos Worldline Xenoa Eco	PTS Approval 4-30097 PTS-approved SCR for UPTs
Atos Worldline Yomani XR/ML, Yomani touch XR/ML	PTS Approval 4-30092 PTS-approved desktop terminal
Atos WorldlineYoximo	PTS Approval 4-30094 PTS-approved handheld payment terminal
Atos WorldlineValina	PTS Approval 4-30222 PTS-approved SCR for UPTs
Spire Payments Holdings S.a.r.l SPm20	PTS Approval 4-20288 PTS-approved handheld payment terminal

Atos Worldline operating systems are

Atos Worldline Samoa	3.6.0
Atos Worldline Spica	4.4.4

Dependent Spire Payments hardware is SPm20 and operating system is Linux 2.6.

Payment Card Core can be used in different configurations:

- integrated with an attended POS
- integrated with an unattended machine like vending machine or parking meter
- standalone

5.3.2 Payment Card Core software dependencies

Poplatek provides the payment application, which runs inside the terminal operating system on the terminals listed above.

For developing the Payment Card Core, SDK from terminal manufacturersis required.

Poplatek payment terminal supports connection to the network with USB or Ethernet wiring or wireless using WLAN, 3G or Bluetooth. When USB is used, Atos provided and supported USB drivers for the hardware listed above must be used.

In addition Payment Card Core requires the following external software components during the software development process and running the Payment Card Core. These components are managed and updated by Poplatek. These software components are linked into the software package and thus delivered as part of the payment terminal SW. Poplatek takes care that these software components are up-to-date e.g. through a vulnerability management and software update processes and procedures: LUA, zlib, lzlib, bitop, lz4, Undescore.lua.

5.3.3 Protocols used by the Poplatek payment terminal SW

Payment Frontend

Poplatek payment terminal SW uses TLS 1.2 with strong cryptography to communicate with the payment frontend on TCP port 443. The payment terminal authenticates the frontend using a Poplatek CA root, while the client is authenticated using OAuth2 tokens. All requests to the frontend are OAuth2-authenticated HTTPS requests which the frontend forwards based on the request URI. The payment terminal uses HTTPS GET/POST requests for e.g. OAuth2 token updates, software update checks, and parameter/file downloads. A Websocket connection, initialized using a HTTPS Upgrade header, is used to carry a JSONRPC connection to the Payment Gateway, providing transaction data transfer, authorizations, and other payment related messaging.

The payment terminal communicates only with the Payment Frontend, except for Worldline Samoa terminal IPKG software update downloads.

POS Protocol for POS integrations

The PA uses Poplatek POS protocol for communicating with the ECR and listens on TCP port 10001. The ECR initiates communication with the PA. The POS protocol never transmits sensitive cardholder data to the ECR, PANs are masked (only the first six and maximum four last digits are shown) for transaction receipt purposes.

Software Updates (Atos Wordlline terminals with Samoa OS)

The Poplatek Payment terminal uses software update service through software updater.

Atos Worldline includes updater software in the production image. This updater connects with mutually authenticated TLS 1.2 on TCP port 443 to the Poplatek update server and downloads package index file, which includes a list of Atos signed ipkg packages to be installed.The software update server provides TLS Certificate signed by Poplatek. The Poplatek payment terminal usespayment terminal internal hardware generated client certificate signed by Atos Worldline. Neither Poplatek nor Atos Worldline have access to the corresponding private key of this client certificate (the private key is used internally by the OS and hardware).

If the package listed in the list is not installed on the payment terminal, the updater installs the package andAtos Samoa OS takes care that the package is properly signed by Atos Worldline. The Atos Worldline Samoa OS does not allow downgrading packets.

The package signature process is completely managed by Atos Worldline. .

Software Updates (Atos Wordlline terminals with Spica OS)

The payment terminal checks for updates and downloads update package(s) using HTTPS GET/POST requests sent to the Payment Frontend which forwards them to the update server. The payment terminal reports its current software versions in an update check request, and the update server response indicates either that software is up-to-date or that specified updates need to be installed. The server is responsible for preventing unintended downgrades.

Atos Spica OS takes care that the package is properly signed by Atos Worldline. The package signature process is completely managed by Atos Worldline.

Software Updates (Spire Payments terminals)

The payment terminal checks for updates and downloads update package(s) using HTTPS GET/POST requests sent to the Payment Frontend which forwards them to the update server. The payment terminal reports its current software versions in an update check request, and the update server response indicates either that software is up-to-date or that specified updates need to be installed. The server is responsible for preventing unintended downgrades.

The update packages are SHA256 hash validated before installation, and the update package format itself contains a digital signature which Spire system software checks before installation. Software update packages are signed by Poplatek using a dual-controlled hardware security device (Spire Signer Device).

Unattended configuration connections

The PA supports RS-232, RFCOMM, TCP, and JSON-RPC to connect to a POS system outside of the PTS-approved terminal. The PA uses different integrations with different unattended machine connections. For example, payment terminal SW may use JSON RPC connection to TCP port 12765 if configured to communicate with a Vending Machine. The apayment terminal SW may use RS232 hardware interface to communicate with an unattended machine with MDB protocol, or even in-house developed protocol to communicate over RS232 to a micro-controller. The unattended protocol never carries any sensitive cardholder data.

5.4 Key Management

Payment terminal key management happens automatically. No user or merchant can have access to the payment terminal keys. There are no settings menu or other inputs to the terminal that would affect the key management. Software updates take care of updating keys, if ever needed. Also, the software updates happen automatically. No user or merchant actions are required.

The payment terminal uses OAuth2 to manage a refresh token and a bearer token. The first OAuth2 refresh token is obtained using an initial token fixed in the software build. When the first refresh token has been successfully taken into use, the initial token is no longer accepted; refresh tokens are then chained so that a new refresh token is fetched using the current refresh token. An administrator may manually allow a token refresh if a terminal loses its token state. The terminal requests for a token update on every boot (every 24h) which may update the refresh token and the bearer token. The bearer token is used for other HTTPS requests such as update checks, payment gateway connection, etc.

Client certificates used in software updates for Atos Worldline terminals with Samoa OS are generated during manufacturing into the payment terminals and validated on the server side for each connection.

The PA DSS scoped Payment Card Core modules uses RSA 2048-bit encryption to encrypt sensitive cardholder data. Only the payment gateway can decrypt the RSA encrypted data. The RSA public key is installed into the terminal from signature verified packet and updated automatically by Poplatek when close to end of crypto period lifetime.

Name	Category	Key length and algorithm	Cryptoperiod	Purpose	Update mechanism
RSA sensitive CHD encryption public key	Insensitive 2048bit RSA public key stored in flash	2048bit RSA	2 years	To encrypt sensitive CHD data for payment gateway and payment terminal filesystem	Automatic secure software update

5.5 Centralized logging

Poplatek payment terminals implement centralized logging into the payment gateway. The centralized logging is based on a reliable event delivery protocol implemented by Poplatek.

Logging is enabled automatically. Interfering with the logging functionality or disabling logs is not allowed and will result in non-compliance with PCI DSS. Note that it is not possible to disable logging from the payment terminal or PA itself.

Merchants can obtain centralized logging events for their payment terminals on request from Poplatek.

- **Merchant actions**: If merchant needs logging data for some of its terminals containing Poplatek PA, contact Poplatek Payments Oy.

6 Troubleshooting procedures

Poplatek will never request Sensitive Authentication Data (SAD) from customers, including e.g. full PAN, in any situation, including possible troubleshooting cases. In some cases masked PAN (first six and last four digits) as printed on transaction receipt may be requested.

7 Appendix A: PCI PA DSS v3 Requirements related to PA DSS Implementation Guide

1.1.4 **N/A** The payment terminal does not store any sensitive authentication data to the persistent flash storage. Also, no version has stored sensitive authentication data..

1.1.5 We do not store sensitive authentication data to log files. We do not receive any data files from customers that contain sensitive authentication data. Also, customers can not change the payment terminal in such a way that it would store sensitive authentication data for logging purposes. Troubleshooting section 6 explains that Poplatek never asks for SAD.

2.1 Payment terminal doesn’t not provide any function that would allow c customer to store CHD.

2.2 Full PAN is not displayed anywhere. PANs in receipts are automatically masked (first six and last four digits). Masked PANs are NOT shown on terminal display. PA do not log full PANs. Masked PAN is generated by replacing PAN middle digits by * character. Number of middle digits and offset for the first middle digit are defined by following rules (PAN digits replaced by dots in examples):

......**********....   20 digits or more, 6 leading and 4 trailing digits

......*********....   19 digits

......******....   16 digits

......*****....   15 digits

......****....   14 digits

......***....   13 digit

************   12 or less, should never happen for PCI relevant cards2.3 **N/A**. Customer do not have any configurable options for rendering cardholder data unreadable. There are no circumstances where customer would be responsible for rendering the PAN unreadable.

2.4 **N/A**. Key management is automatic, no customer actions required. See “Key Management” section.

2.5 **N/A**. Key management is automatic, no customer actions required. See “Key Management” section.

2.5.1-2.5.7 Payment terminal does not generate cryptographic keys and there is no way a customer can enforce the RSA key renewal. This is automatic and Poplatek takes care of it.

2.6 **N/A**. Only key is public key and the key is automatically renewed with no actions from customer required.

3.1 **N/A** Payment application does not use any user accounts, thus, there is no user account logins or authentications. Currently, there are no user configurable settings either.

3.2 **N/A**. Payment application does not use any user accounts, thus, there is no user account logins or authentications. Currently, there are no user configurable settings either. However, strong access control measures must be used in general, accessing the system components.

4.1 **N/A**. There is no user access or administrative access to the payment terminal. Logging is automatically enabled and is necessary for PCI DSS compliance.

4.4 There is no user access or administrative access to the payment terminal. Logging is automatically enabled and is necessary for PCI DSS compliance. There is no way to disable logging from the PA or Payment Terminal. Poplatek provides logs related to the merchants terminal to the merchants on case-by-case request.

5.4.4 See “Versioning scheme for Payment Card Core module” section.

6.1 **N/A**. PA DSS security requirements are followed when configuring WLAN access points. Wireless is configured separately with payment terminal configuration parameters from the centralized registry. See “Wireless LAN ” section.

6.2 **N/A**. Wireless is configured separately with payment terminal configuration parameters from the centralized registry. WEP is not allowed and only strong encryption algorithms are allowed on the payment terminal. In addition to the secure WLAN connection, payment application encrypts sensitive cardholder data with RSA. The encrypted sensitive cardholder data is also transmitted over mutually authenticated TLS 1.2 connection to the payment gateway. Only the payment gateway can decrypt the RSA encrypted cardholder data.

6.3 See “Wireless LAN ” section.

7.2.3 Software updates are automatic, no customer actions required. See chapter 5.3.3 for details.

8.2 Poplatek usesAtos Worldline and Spire Payments payment terminal hardware and software, but also some external software components. See “Payment Application” for more details.

9.1 **N/A**. Payment Card Core runs on the payment terminal. Poplatek payment terminal is connected to the PCI DSS compliant Poplatek payment gateway, which takes care of the transaction processing and storing. Also, payment application does not provide cardholder data anywhere else than for the payment gateway.

10.1 **N/A** Poplatek payment application does not have remote access capabilities.

10.2.1 **N/A**. Poplatek payment terminal SW connects directly and automatically to the Poplatek software update server. Poplatek does not deliver software updates to the merchants or any customers in any other way. For network configuration see “Installation environment“ section.

10.2.3 **N/A** Poplatek payment application does not have remote access capabilities.

11.1 Payment Card Core encrypts cardholder data with RSA-2048 bit by default, no cardholder action is required. The encrypted sensitive cardholder data is automatically transmitted over mutually authenticated TLS 1.2 connection to the payment gateway. Only the payment gateway can decrypt the RSA encrypted cardholder data.

11.2 **N/A**. Payment application does not facilitate the sending of PANs by end-user messaging technologies.

12.1 **N/A** There is no remote or local administrative access implemented for Poplatek apayment terminal. Note also that Payment Card Core related settings come directly from the payment gateway.

12.1.1 **N/A** There is no remote or local administrative access implemented for Poplatek payment terminal. Note also that Payment Card Core related settings come directly from the payment gateway.

12.2 **N/A** There is no remote or local administrative access implemented for Poplatek payment terminal. Note also that Payment Card Core related settings come directly from the payment gateway.