EPS

PA-DSS Implementation Guide

Version 1.5 - 21 January, 2019

CONFIDENTIAL INFORMATION

This document is the property of EPS; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of EPS.

Revision History

Changes	Approving Manager	Date
1.0 - Initial Publication	Nikolaj Goranin	2012 02 05
1.1 – Update for version 1.1013a, correction of minor typing and spelling mistakes.	Nikolaj Goranin	2013 10 14
1.2 – Update for version 1.1218aX recertification according to PA DSS 3.2 requirements.	Nikolaj Goranin	2016 11 11
1.2 – Annual review. No document changes made.	Nikolaj Goranin	2017 12 01
1.2 – Annual review. No document changes made.	Nikolaj Goranin	2018 11 30
1.3 – Introduction of Ingenico TETRA platform.	Nikolaj Goranin	2019 01 04
1.4 – Clarifications, related to user management, software development processes, versioning.	Nikolaj Goranin	2019 01 18
1.5 – Clarifications, related to versioning, minor redactions.	Nikolaj Goranin	2019 01 21

Table of Contents

1 INTRODUCTION AND SCOPE

1.1 Introduction

The purpose of this PA-DSS Implementation Guide is to instruct merchants, resellers and integrators on how to implement EPS's AsyncPOS T Version 1.1218aX into their environment in a PA-DSS compliant manner. It is not intended to be a complete installation guide. AsyncPOS T, if installed according to the guidelines documented here, should facilitate and support a merchant's PCI DSS compliance.

The application can be used with the host supporting EPS developed AsyncPOS protocol.

AsyncPOS T payment application can be installed on Telium 2 or TETRA platform Ingenico PTS device certified according to PTS requirements.

1.2 What is Payment Application Data Security Standard (PA-DSS)?

The Payment Application Data Security Standard (PA-DSS) is a set of security standards that were created by the PCI SSC to guide payment application vendors to develop secure payment applications.

1.3 Distribution and Updates

This PA-DSS Implementation Guide should be disseminated to all relevant application users including merchants, resellers and integrators.

The application is not supposed to be installed by end users, customers. The first installation is performed to the PTS device by application vendor with use of cryptographic signing smartcards. The initial Implementation Guide version is distributed to the client after signing a service agreement.

Implementation guide should be updated in the following cases:

- after annual review, if changes were to the Implementation Guide were made;
- after changes in the software and relevant dependent information systems if appropriate;
- after changes in the PA-DSS standard.

Initial version of Implementation Guide, updates, and updated versions of Implementation Guide documents are distributed to customers via e-mail, web-site or via other agreed communication method or can be obtained by contacting EPS LT, UAB support (support@eps.lt).

1.4 Application Versioning Methodology

The AsyncPOS T application uses the following versioning methodology: N.MMYYa[X], where N stands for numbers, MM – month, YY – year, a – lowercase letter, X – number.

Sample: 1.1218a0001

The first N (1 before dot in sample) marks the general version of application. This number is not supposed to be changed during the application lifecycle. In case application architecture is changed or application lifecycle ends it is increased by 1. In any case it marks major changes towards application architecture and PA-DSS compliance.

MMYY depicts the month and the year when the application High impact change is performed. It is not allowed to perform more than one High impact change towards PA-DSS compliance per month.

a – represents a Low impact change that never represent a security impacting change. Letters are incremented according to Latin alphabet (a, b, c, d...). These changes may have impact on application functionality but no impact on security or PA-DSS requirements.

Wildcards (X) after the letter represent No-impact changes to the application, that also never represent a security impacting change. Continuous numbering is used. Any other elements to the right of a wildcard cannot be used or represent any security-impacting change.

The definitions of changes are defined according to PA-DSS program guide 3.2. Wildcards are never used for any change that has an impact on security or any PA-DSS requirements.

1.5 Standards Versions

This PA-DSS Implementation Guide references both the PA-DSS and PCI DSS requirements. The following versions were referenced in this guide.

- PA-DSS version 3.2
- PCI DSS version 3.2.1

2 SECURE DELETION OF SENSITIVE DATA AND PROTECTION OF STORED CARDHOLDER DATA

2.1 Merchant and Reseller/Integrator Applicability

It is both the merchant's and reseller's or integrator's responsibility to remove any magnetic stripe data, card validation values or codes, PINs or PIN block data, cryptographic key material, or cryptograms stored by previously used software, either installed on the PED devices or ECRs

The AsyncPOS T software itself does not facilitate the storage of sensitive authentication data, PIN block or PIN, this includes normal operation as well as during troubleshooting.

2.2 Secure Deletion Instructions

Merchants, resellers and integrators do not need to purge data stored by previous versions of the AsyncPOS T software. All data in non-volatile memory of POS hardware terminal is purged automatically before new versions are installed.

Prior to a software upgrade the customer performs a Day Close (Check Point) or this procedure is performed automatically which clears the non-volatile memory of any remaining transactions and data. Scheduled updates are pushed to terminals after Check Point is performed.

2.3 Cardholder Data Encryption and Data Retention

AsyncPOS T reads necessary information from card (PAN, Expiration data, Service code (optional, bank-dependant)) and receives PIN if needed and performs authorization (online or offline). Cardholder data and PIN is held in PED volatile memory only in the encrypted form.

AsyncPOS T transmits cardholder data to the EPS host only in the encrypted form, application does not transmit cardholder data to the customer and has no such technical possibility. Encryption cannot be disabled through any setting. Encryption algorithms are hard coded into the application and cannot be changed through configuration either.

Transaction data is encrypted (AES 128-bit) and is sent to EPS host (PAN, Expiration data, Service code (optional, bank-dependant) and encrypted PIN-Block). PED stores encrypted (TripleDES 112-bit) CHD in internal non-volatile memory for approved offline transactions and online transactions, until Check Point with EPS Host is performed (usually once a day or on demand). After transaction is authorized AsyncPOS T will clear the volatile memory of any sensitive authentication data (PIN, Service code, which is optional). After Check Point AsyncPOS T will clear encrypted cardholder data (PAN and Expiration Date) stored in terminals non-volatile memory.

AsyncPOS T transmits cardholder data to the EPS host only in the encrypted form, application does not transmit cardholder data to the customer and has no such technical possibility.

AsyncPOS T uses automatic key management system. All encryption keys are managed by application vendor according to the PCI DSS requirements. Customer or resellers/integrators does not have access to encryption mechanisms and keys at all.

Application encryption keys are not stored anywhere apart from PTS device Secure Area or volatile memory.

Rendering encryption key material in irretrievable form is ensured by means of PTS terminal.

Old keys are rendered irretrievable during re-keying or PTS device re-initialization.

There is no necessity for re-encryption of historical data since each transaction is encrypted with a unique derived key and full CHD will be not relevant after Check Point.

AsyncPOS T does not make use of SSL/TLS technologies for protecting transmitted cardholder data.

Before a software upgrade it is required that the terminal performs Check Point to clear any transaction data stored of the payment terminal.

AsyncPOS T does not store cardholder data to any other location outside the payment terminal, cardholder data can't be extracted outside of the payment terminal.

AsyncPOS T automatically and securely deletes cardholder data when no longer required for legal, regulatory, or business purposes, merchants should only formally inform EPS for defining the business purpose needs on cardholder data storage, if not defined separately, internal EPS data retention policy will be applied, that complies with PCI DSS requirements. Default retention policy is to retain 700 transactions. When retention limits are reached automatic Check Point is performed.

All cardholder data is deleted automatically after Check Point or Day Close is performed. Customer is able to initiate Day Close by himself and data will be deleted automatically.

AsyncPOS T is installed on Ingenico Telium 2 or TETRA platform that does not store card data and there are no other OS, databases.

Merchants should configure any systems connected to or systems used to facilitate transmission of encrypted card data in such a way that capture of encrypted transaction strings is avoided, merchants are instructed to delete any inadvertently captured encrypted transaction strings and not to store them for any reason.

2.4 PAN Masking

AsyncPOS T masks PAN by default on receipts and local transaction log display. If not defined in a different way by the EPS host the first 6 and the last 4 digits of PAN are outputted. The number of digits to be displayed on a receipt / transaction log and the masking sign is defined by EPS via the EPS host.

There is no option to enable troubleshooting options that would display the full PAN on receipts.

Receipts and local transaction logs are the only instances where by default truncated PAN can be seen/displayed.

3 PASSWORD AND ACCOUNT SETTINGS

3.1 Access Control

Merchants, resellers and integrators are advised to control access, via unique username and PCI DSS compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

AsyncPOS T does not have any user accounts and does not allow user access. There is no user access to card data as well, application does not manage or generate user accounts.

The only access possible is through the configuration menu on the payment terminal. These menu can not be used for changing application security parameters, accessing / reviewing cardholder data and is only for specifying the connection type (Ethernet, Wi-Fi, GPRS or RS232) and performing maintenance actions (e.g. end-of-the-day).

AsyncPOS T usage does not require from the merchant to access PCs, servers, and databases.

3.2 Passwords

General PCI DSS password requirements are as follows and should be used on any system that stores, processes or transmits cardholder data: Passwords should meet the requirements set in PCI DSS section 8.2.3 through 8.2.6, as listed here.

- Do not use group, shared, generic or default accounts and passwords
- Change user passwords at least every 90 days
- Require a minimum password length of at least seven characters
- Use passwords containing both numeric and alphabetic characters
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used
- Limit repeated access attempts by locking out the user ID after not more than 6 attempts
- Set the lockout duration to thirty minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal

4 LOGGING

4.1 Merchant Applicability

Currently, for EPS's AsyncPOS T version 1.1218aX, there are no end-user, configurable, logging settings. All logging settings, such as application maintenance from EPS side, system-level object management, transactions, etc. are defined by EPS host to conform to PCI DSS logging requirements.

No local logs, that would display cardholder data, could be enabled neither via configuration interface, nor via host.

The only local log can display truncated PAN only and other technical transaction data.

There are no user/administrator accounts used and there are no corresponding logs / audit trails utilized. Due to that there are no logs and centralized logging is not applicable.

4.2 PCI Guidelines for Logging

Implement automated audit trails for all system components to reconstruct the following events:

- All individual accesses to cardholder data.
- All actions taken by any individual with root or administrative privileges.
- Access to all audit trails.
- Invalid logical access attempts.
- Use of identification and authentication mechanisms.
- Initialization of the audit logs.
- Creation and deletion of system-level objects.

Record at least the following audit trail entries for all system components for each event:

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

4.3 Configuring Log Settings

Applicable and technologically possible logs (application maintenance from EPS side, system-level object management, local transaction logs) are enabled out of the box and can't be disabled; disabling logging will make the product non-compliant with PCI DSS.

There are no user/administrator accounts used and there are no corresponding logs / audit trails utilized.

5 WIRELESS NETWORKS

5.1 Merchant Applicability

AsyncPOS T encrypts cardholder data and transaction strings at the point of entry in the payment terminal and sends the data encrypted to EPS LT, UAB, for decryption and processing. The application does not rely on any specific communication type for delivery of transactions to EPS LT, UAB.

However, if wireless is used or implemented in the environment, the wireless environment must be configured to meet PCI DSS requirements. Wireless technology must be securely implemented and transmissions of cardholder data over wireless networks must be secure.

This is only applicable if cardholder data is sent over wireless networks; this does not include transactions sent by the AsyncPOS T software.

5.2 PCI Requirements

Although the security of cardholder data, processed by AsyncPOS T is ensured by the application level encryption, and is not dependent on the external transport technologies used by the merchant it is recommended to implement the following PCI DSS requirements, related to the wireless technology usage in the merchants environment to minimize the overall risk:

- Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.
- For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Wireless encryption keys, passwords and SNMP strings must be changed anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.
- Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.

6 NETWORK SEGMENTATION

6.1 Merchant Applicability

AsyncPOS T does not store cardholder data outside of the payment terminals, if cardholder data is stored anywhere else by any other application, the following requirements apply:

Credit card data cannot be stored on systems directly connected to the Internet. For example, web servers and database servers should not be installed on the same server. A DMZ must be set up to segment the network so that only machines on the DMZ are Internet accessible.

7 SECURE REMOTE SOFTWARE UPDATES

7.1 Merchant Applicability

EPS securely delivers remote payment applications by automatic application upload to the PED device from EPS host, cryptographically signed with the help of Ingenico delivered SMART cards and by applying split knowledge principles, encrypted and additionally CRC checked, there is no user interaction or remote human access required during the update process.

Remote connection, such as VPN, into Client network is not required for update. Update is performed over already existing established communication channel used for normal terminal operations.

Merchant can formally specify in the SLA the preferred automatic update time, agree on the piloting for the updated AsyncPOS T version prior to the update of all terminals. This is applied only to the updates that are not security critical. The latter ones are delivered immediately after the formal release.

8 MINIMUM TECHNICAL REQUIREMENTS

8.1 Merchant Applicability

AsyncPOS T uses only necessary and secure services, protocols, daemons, components and dependent software, approved and certified by the Ingenico terminal vendor. For normal operation AsyncPOS T requires:

- Ingenico Telium 2 or TETRA PTS approved device.
- TCP/IP connection to EPS premises.
- Open outbound TCP port 2223 on client's network infrastructure.

9 REMOTE ACCESS

9.1 Merchant Applicability

AsyncPOS T does not have any user accounts and does not allow remote user access; the only access possible is through the configuration menu on the payment terminal.

AsyncPOS T does not facilitate remote user access.

10 ENCRYPTING NETWORK TRAFFIC

10.1 Transmission of Cardholder data

The AsyncPOS T uses AES 128-bit DUKPT encryption for transmission of cardholder data over public networks.

Users are not able of changing the communication method or encryption settings of the AsyncPOS T.

The AsyncPOS T requires an Internet connection either through the ECR or on a separate connection (Ethernet, Wi-Fi, GPRS) to communicate with the central EPS host.

10.2 Message and cardholder data encryption

All messages sent to and from the AsyncPOS T is encrypted using AES 128-bit DUKPT, encrypting both the message and the data with separate keys, achieving double encryption for all data sent to and from the EPS host.

10.3 Email and Cardholder data

AsyncPOS T does not support the sending information via end-user messaging technologies. Cardholder data should never be sent unencrypted via end-user messaging technologies.