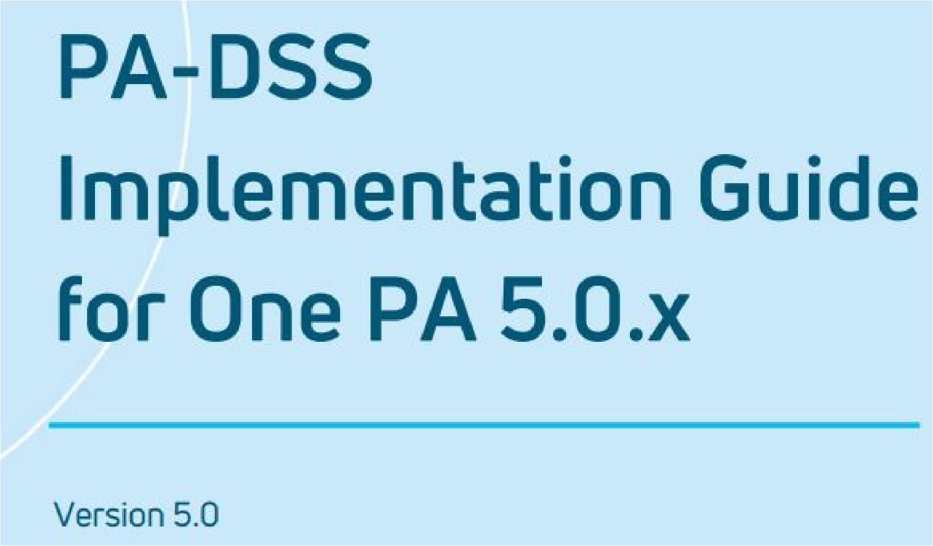
nets PA-DSS One PA 5.0.x User Guide

nets PA-DSS One PA 5.0.x User Guide



PA-DSS
Implementation Guide
for One PA 5.0.x

Version 5.0

Contents [hide

Introduction and Scope

Introduction

The purpose of this PA-DSS Implementation Guide is to instruct Merchants on how to implement Nets' One PA application into their environment in a PCI DSS compliant manner. It is not intended to be a complete installation guide. One PA, if installed according to the guidelines documented here, should facilitate and support a merchant's PCI compliance.

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 implement secure payment applications.

Distribution and Updates

This PA-DSS Implementation Guide should be disseminated to all relevant application users including merchants. It should be updated at least annually and after changes in the software. The annual review and update should include new software changes as well as changes in the PA-DSS standard. Updates to the PA-DSS Implementation Guide can be obtained by contacting Nets directly. 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

Locations of displayed and printed out PANs (PA-DSS v3.2, Appendix A: 2.2)

One PA payment application will display or print out truncated or encrypted Primary Account Number in the following cases:

- Cardholder receipt is printed for online and offline approved purchases, refunds and reversals: truncated PAN, where the last 4 digits are visible
- Merchant receipt is printed for online approved purchases, refunds and reversals: truncated PAN, where the 6 first and the 4 last digits are visible
- Merchant receipt is printed for offline approved purchases: truncated PAN, where the 6 first and the 4 last digits are visible. In addition, encrypted PAN, expiry date and timestamp will be printed.
- Copy of the receipt of the last approved transaction: merchant and cardholder receipts may be printed, depending on if they were printed for the original transaction. Merchant having the 6 first and the 4 last digits are visible. Customer having the last 4 digits visible.
- Copy of the receipt of the last transaction: merchant and cardholder receipts may be printed, depending on if they were printed for the original transaction. Merchant having the 6 first and the 4 last digits are visible. Customer having the last 4 digits visible.
- Transaction list of the current batch: declined and approved transactions where PAN may or may not be printed for declined transactions and will be printed for approved transactions. If PAN is printed, 6 first and the 4 last digits will be visible, and rest of the digits will be truncated.
- Transaction list of the previous batch: declined and approved transactions where PAN may or may not be printed for declined transactions and will be printed for approved transactions. If PAN is printed, 6 first and the 4 last digits will be visible, and rest of the digits will be truncated.
- Reversal of the previous transaction: truncated PAN, where the 6 first and the 4 last digits are visible will be displayed on terminal screen.

There is no user configuration for displaying or printing out PAN and One PA payment application will never display or print out non-truncated or unencrypted PAN.

Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data (PA-DSS v3.2, Appendix A: 1.1.4, 1.1.5, 2.1, 2.4, 2.5, 2.6)

Merchant Applicability (PA-DSS v3.2, Appendix A: 1.1.4)

It is the Merchants responsibility to remove any magnetic stripe data, card validation values or codes, PINs or PIN block data, cryptographic key material, or cryptograms stored by previous versions of the payment application software. However, for the One PA application this is not necessary as none of these items are present. To be PCI compliant, a merchant must have a data-retention policy which defines how long cardholder data will be kept. One PA does not retain cardholder data and can be exempt from the merchant's cardholder data-retention policy. One PA has no functions, settings or configuration options that allow users to change the retention or retention period of sensitive data either in transient or permanent memory.

Secure Delete Instructions (PA-DSS v3.2, Appendix A: 2.1)

The following process is used by One PA to automatically and securely delete prohibited historical data and to purge cardholder data after expiration: The terminal does never store sensitive unencrypted authentication data; CVC, CVV or PIN, neither before or after authorization. Any instance of prohibited historical data that exists in a terminal will be automatically deleted securely when One PA payment application is installed on the terminal. Deletion of prohibited historical data and data that is past retention policy will happen automatically.

Locations of Stored Cardholder Data (PA-DSS v3.2, Appendix A: 2.3)

Cardholder data is stored in the flash system of the terminal in case of:

- Transaction was offline approved. The transaction will be saved as 3DES encrypted. Offline transactions will be deleted from the flash system of the terminal after successfully received by Nets host.
- Any approved purchase or refund. The previous approved transaction will be stored as truncated Track2 (Last 4 digits of PAN) and truncated PAN (last 4 digits of PAN), until the next approved or declined transaction, so that reversal of the previous purchase can be done.

The data is not directly accessible by the merchant.
Cardholder data is never stored in ECR for ECR integrated payment terminals.

Troubleshooting Procedures (PA-DSS v3.2, Appendix A: 1.1.5)

When troubleshooting issues, care must be taken to properly protect cardholder data: Collect sensitive authentication data 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. Nets support will not request sensitive authentication or cardholder data for troubleshooting purposes.

Key management (PA-DSS v3.2, Appendix A: 2.4, 2.5, 2.6)

For the range of all terminal models (Telium Tetra and Spire), all security functionality is performed in a secure area protected from the payment application. Encryption is performed within the secure area while decryption of the encrypted data can only be performed by the Nets Host systems. Procedures for Key Management are implemented by Nets according to a DUKPT scheme using 3DES. The key management is independent of the payment functionality. Loading a new application therefore does not require a change to the key functionality. When the key space is exhausted, the terminal has to be replaced.

Password and Account Settings (PA-DSS v3.2, Appendix A:3.1, 3.2)

Access Control (PA-DSS v3.2, Appendix A: 3.1, 3.2)

The One PA payment application does not have user accounts, so there are no corresponding passwords.

Password Controls (PA-DSS v3.2, Appendix A: 3.1, 3.2)

The One PA payment application does not have user accounts or corresponding passwords; therefore, the One PA application is exempt from this requirement. However, for the merchants general knowledge listed below are the PCI password requirements.

- Customers are advised against using administrative accounts for application logins (e.g., don’t use the “sa” account for application access to the database).
- Customers are advised to assign strong passwords to these default accounts (even if they won’t be used), and then disable or do not use the accounts. Customers are advised to assign strong application and system passwords whenever possible.
- Customers are advised how to create PCI DSS-compliant complex passwords to access the payment application. Customers 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.

Passwords should meet the requirements as shown below:

- Do not use group, shared, or generic 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.

Logging (PA-DSS v3.2, Appendix A: 4.1, 4.4)

Merchant Applicability (PA-DSS v3.2, Appendix A: 4.1)

Currently, for Nets One PA payment application, there is no end-user, configurable PCI log settings.

Configure Log Settings (PA-DSS v3.2, Appendix A: 4.1)

The One PA payment application does not have user accounts, so PCI compliant logging is not applicable. Even in the most verbose transaction logging the One PA application does not log any sensitive authentication data or cardholder data.

Central Logging (PA-DSS v3.2, Appendix A: 4.4)

The terminal has a generic log mechanism.

Crash Logs (PA-DSS v3.2, Appendix A: 4.1)

The terminal logs software crashes and reboot events for quality improvement purposes. The logs do not contain any sensitive or cardholder data. Those logs are automatically sent to Nets host within 10 minutes after terminal has rebooted.

Secure Payment Application (PA-DSS v3.2, Appendix A: 8.2)

Application SW (PA-DSS v3.2, Appendix A: 8.2)

The One PA terminal application does not use any external SW and HW not belonging to the One PA embedded application. All SW executables belonging to the embedded system are digitally signed. The terminal communicates with the Nets Host using TCP/IP, either via Ethernet, USB, GPRS, 3G or 4G technologies. The terminal always takes the initiative for establishing the communication towards the Nets Host. There is no TCP/IP server SW in the terminal, and the terminal SW is never responding to incoming calls. The application protocol (and applied encryption) is transparent and independent of the type of communication. One PA does not require user interaction to configure the cryptographic methods used to protect sensitive data. The payment application does not rely on software settings or values to mitigate vulnerabilities.

Wireless (WLAN) Networks (PA-DSS v3.2, Appendix A: 6.1, 6.2, 6.3)

Merchant Applicability (PA-DSS v3.2, Appendix A: 6.1, 6.2)

One PA does not make use of Wireless Local Area Network (WLAN) technology. However, the use of WLAN is possible together with One PA, in order for it to be implemented securely, consideration should be taken when installing and configuring the wireless network as detailed below.

Recommended Wireless Configurations (PA-DSS v3.2, Appendix A: 6.3)

There are a number of considerations and steps to take when configuring wireless networks that are connected to the internal network. At a minimum, the following settings and configurations must be in place:

- All wireless networks must be segmented using a firewall, if connections between the wireless network and the cardholder data environment is required the access must be controlled and secured by the firewall.
- Change the default SSID and disable SSID broadcast
- Change default passwords both for wireless connections and wireless access points, this includes console access as well as SNMP community strings
- Change any other security defaults provided or set by the vendor
- Ensure that wireless access points are updated to the latest firmware
- Only use WPA or WPA2 with strong keys, WEP is prohibited and must never be used
- Change WPA/WPA2 keys at installation as well as on a regular basis and whenever a person with knowledge of the keys leaves the company

Network Segmentation (PA-DSS v3.2, Appendix A: 9.1)

Merchant Applicability

The One PA payment application is not a server-based payment application and resides on a terminal. For this reason, the payment application does not require any adjustment to meet this requirement. For the merchant’s general knowledge, 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.

Secure Remote Software Updates (PA-DSS v3.2, Appendix A:10.2.1, 10.2.3, 7.2.3)

Merchant Applicability (PA-DSS v3.2, Appendix A: 10.2.1, 10.2.3, 7.2.3) Nets securely deliver remote payment applications updates, using DUKPT MAC signed algorithm. These updates occur on the same communication channel as the secure payment transactions, and the merchant is not required to make any changes to this communication path for compliance. For general information, merchants should develop an acceptable use policy for critical employee-facing technologies, per the guidelines below for VPN, or other highspeed connections, updates are received through a firewall or personal firewall.

- Use a firewall if the computer is connected via VPN or other high-speed connection, and to secure these connections by limiting only the sockets necessary for the application to function.
- Only activate remote access when needed and immediately inactivate after use.

Acceptable Use Policy

The merchant should develop usage policies for critical employee-facing technologies, like modems and wireless devices. These usage policies should include:

- Explicit management approval for use.
- Authentication for use.
- A list of all devices and personnel with access.
- Labelling the devices with owner.
- Contact information and purpose.
- Acceptable uses of the technology.
- Acceptable network locations for the technologies.
- A list of company approved products.
- Allowing use of modems for vendors only when needed and deactivation after use.
- Prohibition of storage of cardholder data onto local media when remotely connected.

Personal Firewall (PA-DSS v3.2, Appendix A: 10.2.3)

Any “always-on” connections from a computer to a VPN or other high-speed connection should be secured by using a personal firewall product. The firewall is configured by the organization to meet specific standards and not alterable by the employee.

Remote Update Procedures (PA-DSS v3.2, Appendix A: 10.2.3, 7.2.3)

There is two ways an update for a terminal can be triggered: manual and scheduled.
A manual trigger is used for the terminal to contact Nets software center: via a menu choice in the terminal (select menu 0 “Settings”, 2 “Check for updates”).
For a scheduled trigger, terminal receives a management plan from MS-TMS. According to a management plan schedule, terminal will automatically contact Nets software center.
After a successful software update, a terminal with a built-in printer will print a receipt with information on the new version, containing an URL to the implementation guide and the latest release notes. When updating terminals without printers, terminal integrators will have the responsibility of informing merchants of the update, including the link to the updated implementation guide and the release notes.
In addition to receipt after software update, One PA software version can be also validated via menu choice in the

terminal (select menu 0 “Settings”, 8 “Configuration info”).

Remote Access (PA-DSS v3.2, Appendix A: 10.1)

Merchant Applicability

One PA cannot be accessed remotely. Remote support only occurs between a Nets support staff member and the merchant over the phone or by Nets directly onsite with the merchant.

Remote Access Software Security Configuration

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 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.

Transmission of Cardholder Data (PA-DSS v3.2, Appendix A: 11.1, 11.2, 12.1, 12.2)

Transmission of Cardholder Data (PA-DSS v3.2, Appendix A: 11.1, 11.2)

One PA utilizes the DUKPT, Derived Unique Key per Transaction 3DES encryption for transmission of cardholder data over public networks.

Email and Cardholder Data

One PA does not natively support the sending of email. Cardholder data should never be sent unencrypted via email.

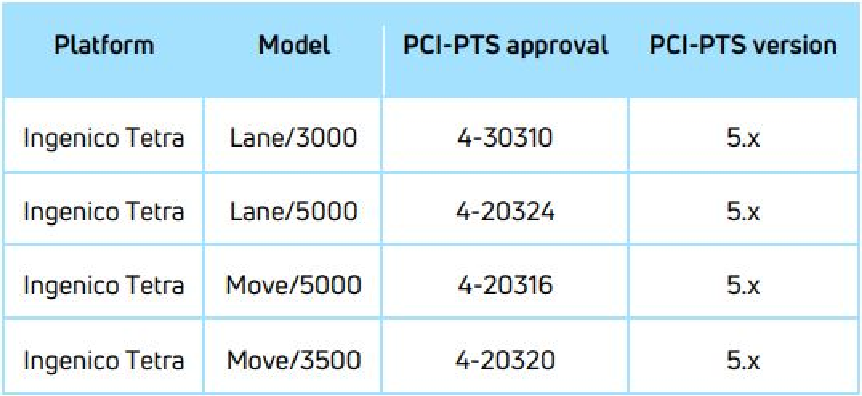
Non-Console Administrative Access (PA-DSS v3.2, Appendix A: 12.1, 12.2)

One PA does not support Non-Console administrative access. However, for the merchants general knowledge, NonConsole administrative access must use either SSH, VPN, or TLS for encryption of all non-console administrative access to servers in cardholder data environment. Telnet or other non-encrypted access methods must not be used.

Hardware, software and network dependencies

Hardware dependencies

One PA payment application supports the following hardware:



Platform	Model	PCI-PTS approval	PCI-PTS version
Ingenico Tetra	Lane/3000	4-30310	5.x
Ingenico Tetra	Lane/5000	4-20324	5.x
Ingenico Tetra	Move/5000	4-20316	5.x
Ingenico Tetra	Move/3500	4-20320	5.x

Software dependencies

The One PA payment application version 5.0.x.

Network dependencies

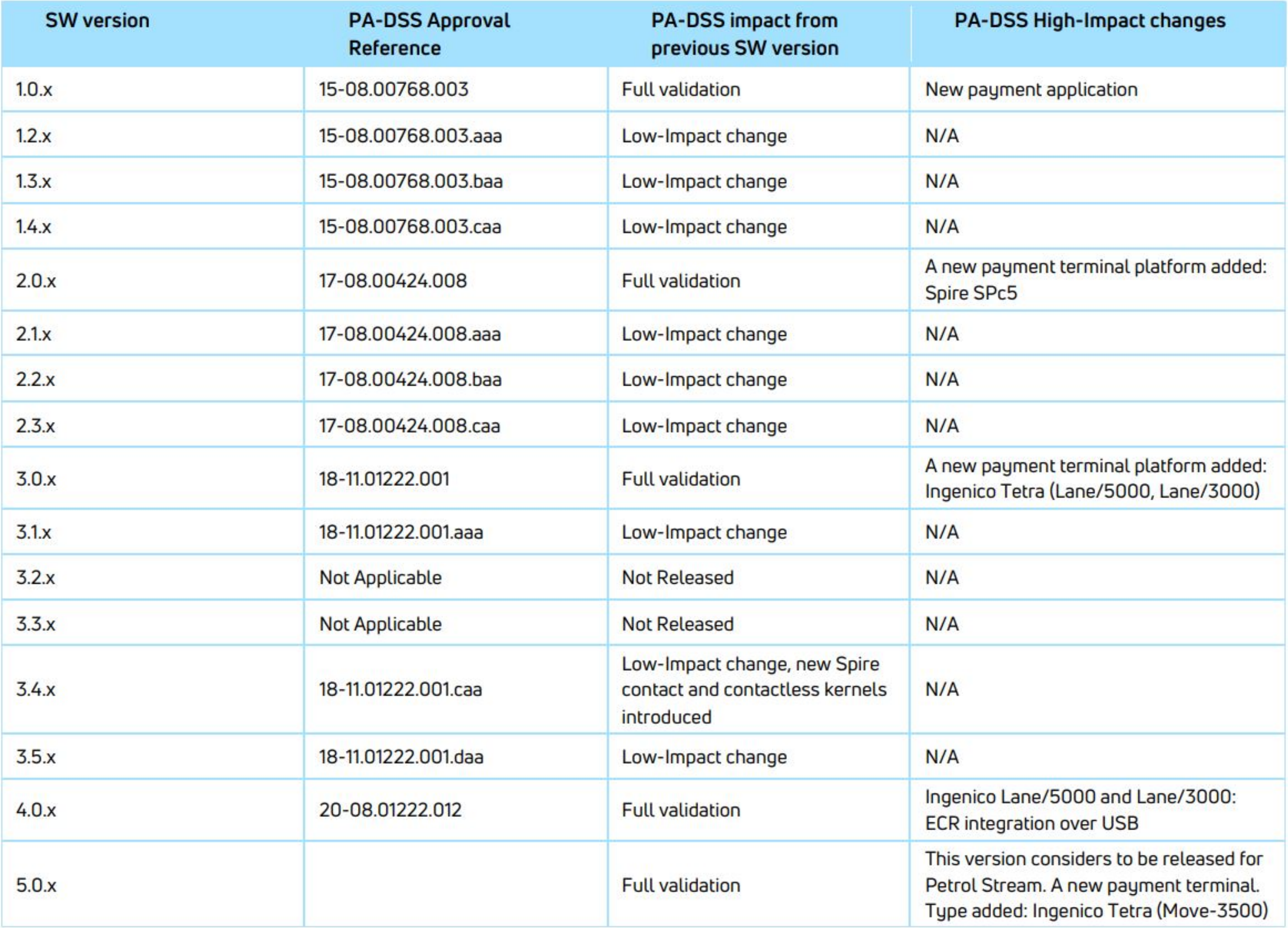
Terminal – Outbound to Nets Host – TCP/9670
Terminal – Outbound to ECR – TCP/6001

One PA Versioning Methodology and PA-DSS Impact (PA-DSS v3.2, Appendix A: 5.4.4)

The Nets versioning methodology consists of a three-part SW version number: n.m.x. The One PA SW version number is shown like this on the terminal screen when the terminal is powered up: Version n.m.x

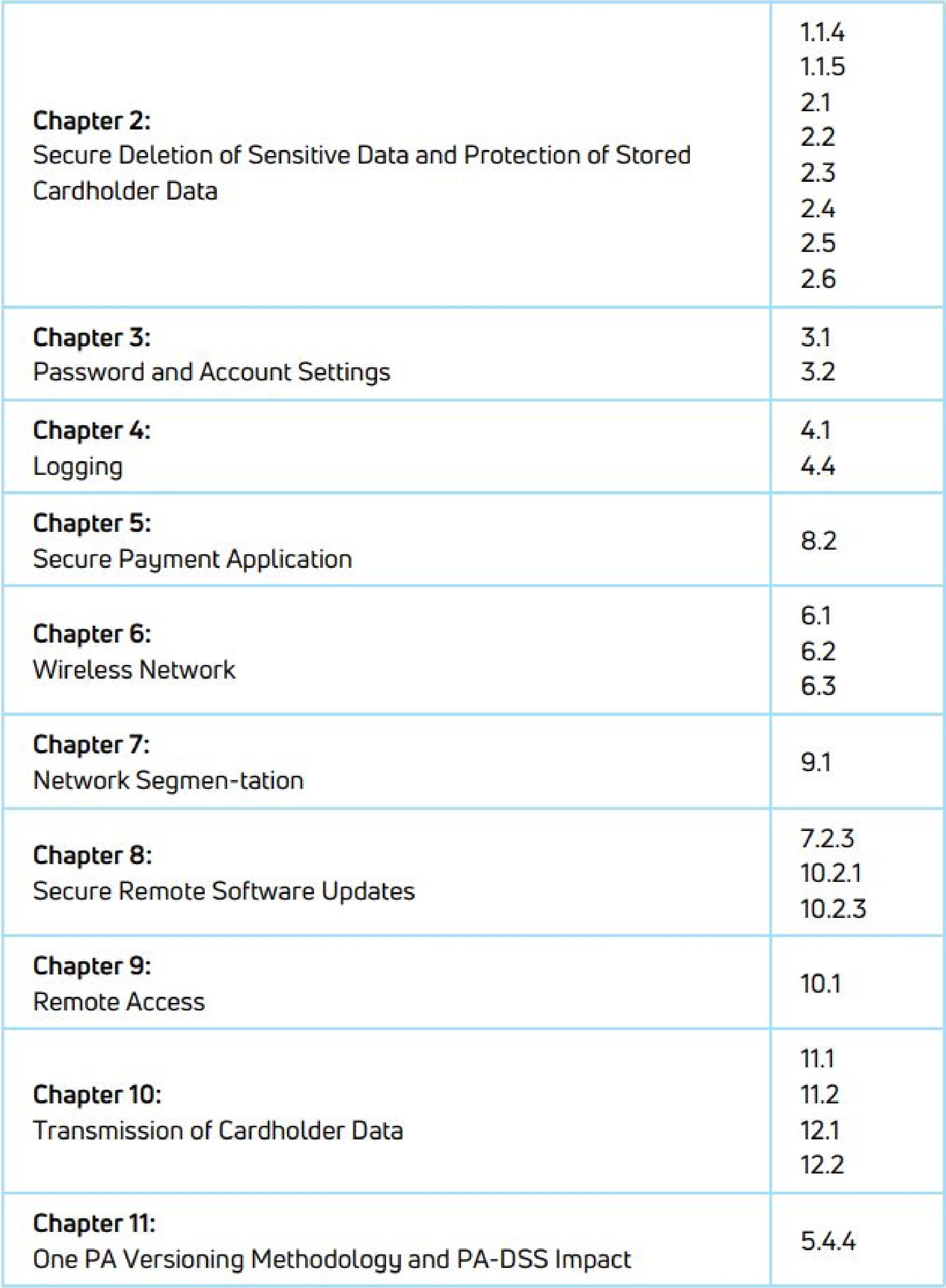
- An update from e.g. 1.0.1 to 1.0.2 is a non-significant functional update. It may not include changes with impact on security or PA-DSS requirements.
- An update from e.g. 1.0.0 to 1.1.0 (1.0.x to 1.1.x) is a non-significant functional update. It may include changes with impact on security or PADSS requirements.
- An update from e.g. 1.0.0 to 2.0.0 (1.0.x to 2.0.x) is a significant functional update. It may include changes with impact on security or PADSS requirements.

The x is the only wildcard component of the SW version number and represents a non-significant update used for a maintenance release. A change in this number will indicate a maintenance release with changes from the previous release without any impact on security or PA-DSS requirements. The PA-DSS change impact level from the previous SW version is described in the table below; the table will be updated for every SW release in the process of updating the Implementation Guide.



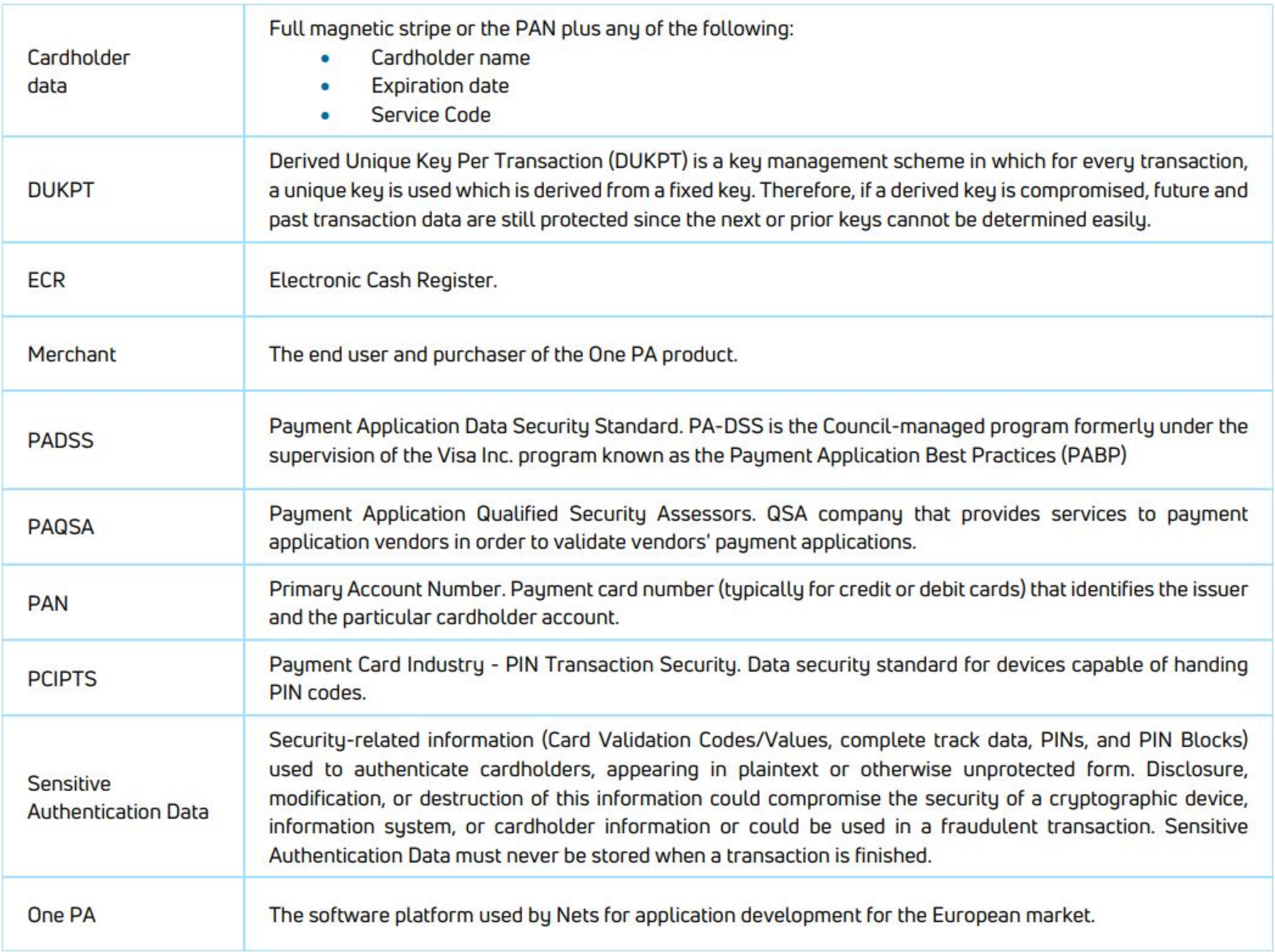
SW version	PA-DSS Approval Reference	PA-DSS impact from previous SW version	PA-DSS High-Impact changes
1.0.x	15-08.00768.003	Full validation	New payment application
1.2.x	15-08.00768.003.aaa	Low-Impact change	N/A
1.3.x	15-08.00768.003.baa	Low-Impact change	N/A
1.4.x	15-08.00768.003.caa	Low-Impact change	N/A
2.0.x	17-08.00424.008	Full validation	A new payment terminal platform added: Spire SPc5
2.1.x	17-08.00424.008.aaa	Low-Impact change	N/A
2.2.x	17-08.00424.008.baa	Low-Impact change	N/A
2.3.x	17-08.00424.008.caa	Low-Impact change	N/A
3.0.x	18-11.01222.001	Full validation	A new payment terminal platform added: Ingenico Tetra (Lane/5000, Lane/3000)
3.1.x	18-11.01222.001.aaa	Low-Impact change	N/A
3.2.x	Not Applicable	Not Released	N/A
3.3.x	Not Applicable	Not Released	N/A
3.4.x	18-11.01222.001.caa	Low-Impact change, new Spire contact and contactless kernels introduced	N/A
3.5.x	18-11.01222.001.daa	Low-Impact change	N/A
4.0.x	20-08.01222.012	Full validation	Ingenico Lane/5000 and Lane/3000: ECR integration over USB
5.0.x		Full validation	This version considers to be released for Petrol Stream. A new payment terminal. Type added: Ingenico Tetra (Move-3500)

PA-DSS Approval Reference



Chapter 2: Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data	1.1.4 1.1.5 2.1 2.2 2.3 2.4 2.5 2.6
Chapter 3: Password and Account Settings	3.1 3.2
Chapter 4: Logging	4.1 4.4
Chapter 5: Secure Payment Application	8.2
Chapter 6: Wireless Network	6.1 6.2 6.3
Chapter 7: Network Segmen-tation	9.1
Chapter 8: Secure Remote Software Updates	7.2.3 10.2.1 10.2.3
Chapter 9: Remote Access	10.1
Chapter 10: Transmission of Cardholder Data	11.1 11.2 12.1 12.2
Chapter 11: One PA Versioning Methodology and PA-DSS Impact	5.4.4

Glossary of Terms



Cardholder data	Full magnetic stripe or the PAN plus any of the following: • Cardholder name • Expiration date • Service Code
DUKPT	Derived Unique Key Per Transaction (DUKPT) is a key management scheme in which for every transaction, a unique key is used which is derived from a fixed key. Therefore, if a derived key is compromised, future and past transaction data are still protected since the next or prior keys cannot be determined easily.
ECR	Electronic Cash Register.
Merchant	The end user and purchaser of the One PA product.
PADSS	Payment Application Data Security Standard. PA-DSS is the Council-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP)
PAQSA	Payment Application Qualified Security Assessors. QSA company that provides services to payment application vendors in order to validate vendors' payment applications.
PAN	Primary Account Number. Payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
PCIPTS	Payment Card Industry - PIN Transaction Security. Data security standard for devices capable of handing PIN codes.
Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction. Sensitive Authentication Data must never be stored when a transaction is finished.
One PA	The software platform used by Nets for application development for the European market.

Document Control

Version Number	Version Date	Nature of Change	Change Author	Date Approved
1.0	17.7.2015	New document based on Viking implementation guide	Jussi Rautio	
1.1	4.8.2015	Updated according to feedback from PA-DSS assessment	Mikko Kohonen	
1.2	9.8.2015	Changed PA-DSS into PCI DSS in Ch.1.1, Deleted host-initiated trigger from Ch. 8.4. Changed PCI DSS version as 3.1, some minor typographical fixes	Mikko Kohonen	
1.3	10.2.2016	Updated document and application versions	Mikko Kohonen	
1.4	3.3.2016	Updated document and application versions	Mikko Kohonen	
1.5	22.9.2016	Updated chapters One PA Versioning Methodology and PA-DSS Impact and Document Control	Mikko Kohonen	
1.6	28.10.2016	Updated PA-DSS Approval Reference for v1.4.x, fixed correct year for summary of changes	Mikko Kohonen	
1.7	10.4.2017	Updated chapters Introduction and Scope, One PA Versioning Methodology and PA-DSS Impact, Logging and Secure Remote Software Updates	Mikko Kohonen	
1.8	12.4.2017	Small review changes	Jussi Rautio	
1.9	4.5.2017	Small changes based on v2.0.x full PA-DSS review meeting	Mikko Kohonen	
2.0	26.9.2017	Table of contents and headers directly refers to PA-DSS Appendix A	Mikko Kohonen	
2.1	21.11.2017	IG One PA Versioning Methodology and PA-DSS Impact	Mikko Kohonen	
2.2	24.11.2017	IG One PA Versioning Methodology and PA-DSS Impact	Mikko Kohonen	
2.3	24.11.2017	Minor changes in IG Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data, IG Secure Remote Software Updates and IG One PA Versioning Methodology and PA-DSS Impact	Mikko Kohonen	
3.0	29.6.2018	Minor changes in IG One PA Versioning Methodology and PA-DSS Impact	Mikko Kohonen	
3.1	30.8.2018	Updated chapter: Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data, Locations of Stored Cardholder Data:added the actual use cases where cardholder data is stored Updated chapter: Glossary of Terms Added a new chapter: Locations of displayed and printed out PANs Added a new chapter: Hardware, software and network dependencies	Mikko Kohonen	
3.2	10.9.2018	Minor changes	Mikko Kohonen	
3.3	12.11.2018	Updated chapters: IG Remote Software Updates, Document control (product owner name)	Jussi Rautio Mikko Kohonen	

3.4	20.11.2018	Updated chapters: Document control, IG One PA Versioning Methodology and PA-DSS Impact, IG Hardware, software and network dependencies	Lidia Ungureanu	
3.5	27.11.2018	Updated chapters: Document control, Secure Remote Software Updates	Lidia Ungureanu	
3.6	18.12.2018	Updated chapters: Document control, IG Logging, Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data	Mikko Kohonen	
3.7	20.12.2018	Updated chapters: Document control, Secure Remote Software Updates	Mikko Kohonen	
3.8	21.12.2018	Updated chapters: Document control, Secure Remote Software Updates	Mikko Kohonen	
3.9	10.1.2019	Updated chapter: Hardware, software and network dependencies	Mikko Kohonen	
3.10	14.2.2019	Updated chapters: Locations of displayed and printed out PANs, Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data	Mikko Kohonen	
3.11	25.2.2019	Updated chapters: Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data	Mikko Kohonen	
3.12	30.4.2019	Updated chapters: Document control, One PA Versioning Methodology	Mikko Kohonen	
3.13	20.5.2019	Updated chapters: Document control, Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data	Mikko Kohonen	
3.14	29.11.2019	Updated chapters: Document control, One PA Versioning Methodology and PA-DSS Impact	Mikko Kohonen	
3.15	17.12.2019	Updated chapters: Document control, One PA Versioning Methodology and PA-DSS Impact	Mikko Kohonen	
3.16	20.1.2020	Updated chapters: Document control, One PA Versioning Methodology and PA-DSS Impact, Hardware, software and network dependencies, Introduction and Scope	Mikko Kohonen	
3.17	22.1.2020	Updated chapters: Document control, Hardware, software and network dependencies, One PA Versioning Methodology and PA-DSS Impact	Mikko Kohonen	
4.0	16.4.2020	Updated chapters: Document control, Hardware, software and network dependencies, One PA Versioning Methodology and PA-DSS Impact, Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data, Secure Payment Application	Mikko Kohonen	
4.1	3.7.2020	Updated chapters: Document control, Introduction and Scope, Locations of displayed and printed out PANs, Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data, Secure Remote Software Updates, PA-DSS Requirements Reference, One PA Versioning Methodology and PA-DSS Impact	Mikko Kohonen	
4.2	19.11.2020	Updated chapters: Document control, One PA Versioning Methodology and PA-DSS Impact	Mikko Kohonen	
5.0	10.2.2021	Updated chapters: Document control, Hardware software and network dependencies, One PA Versioning Methodology and PA-DSS Impact, Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data, Secure Payment Application, Secure Remote Software Updates	Manish Angre	

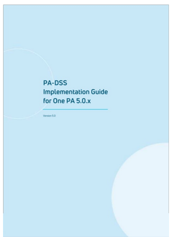
Distribution List

Name	Function
Terminal Department	Development, Test, Project Management, Compliance
Product Management	Terminal Product Management Team, Compliance Manager – Product

Document Approvals

Name	Function
Alexandru Manta	Product Owner

Documents / Resources

 PA-DSS Implementation Guide for One PA 5.0.x Version 5.0	nets PA-DSS One PA 5.0.x [pdf] User Guide PA-DSS One PA 5.0.x, PA-DSS, PA-DSS PA 5.0.x, One PA 5.0.x, PA 5.0.x