Nets Denmark A/S, Finnish Branch:
PA-DSS Implementation Guide for Viking 6.4.x

Version 4.6

Contents

1 Introduction and Scope

1.1 Introduction

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

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 implement secure payment applications.

1.3 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 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 Applicability

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 Viking software. However, for the Viking 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.

Viking does retain cardholder data of the very last transaction and in case if there are offline transactions while adhering to the PADSS compliance at the same time, hence it can be exempt from the merchant's cardholder data-retention policy.

2.2 Secure Delete Instructions

The following process is used by Viking to automatically and securely delete prohibited historical data and to purge cardholder data after expiration:

The terminal does never store sensitive authentication data; CVC, CVV or PIN, neither before nor after authorization.

Any instance of prohibited historical data that exists in a terminal will be automatically deleted securely when the terminal Viking payment application is upgraded. Deletion of prohibited historical data and data that is past retention policy will happen automatically.

2.3 Locations of Stored Cardholder Data

Cardholder data is stored in the Flash DFS (Data File System) of the terminal. Each application has a dedicated part of the DFS which is not accessible by other applications in the terminal. The data is not directly accessible by the merchant.

2.4 Troubleshooting Procedures

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.

2.5 Key management

For the Telium 2 range of terminal models, 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. The terminal key space will support around 2,097,152 transactions. When the key space is exhausted, Viking terminal stops working and shows an error message, then the terminal must be replaced.

2.6 PAN displayed or printed locations

Masked PAN:

- Financial Transaction receipts:
  Masked PAN is always printed on the transaction receipt for both cardholder and merchant. The masked PAN in most of the cases is last 4 digits.
- Transaction list report:
  Transaction list report shows the transactions performed in a session. Transaction details includes Masked PAN, Card issuer name and the transaction amount.
- Last customer receipt copy:
  The copy of last customer receipt can be generated from terminal menu. The customer receipt contains the masked PAN as the original customer receipt. The given function is used in case if terminal fails to generate a customer receipt during the transaction for any reason.

Encrypted PAN:

- Offline transaction receipt:
  Retailer receipt version of offline transaction includes Triple DES 128-bit DUKPT encrypted cardholder data (PAN, Expiry date and Service code).

Confirmation:

Viking PA always encrypts the cardholder data by default for offline transaction storage, transmission towards NETS host and to print encrypted card data on the retailer receipt for an offline transaction.

Also to display or to print the card PAN, Viking PA always masks the PAN digits with asterisk '*' with First 6 + Last 4 digits in clear as default. The card number print format is controlled by terminal management system where print format can be changed by requesting through proper channel and by presenting a business legitimate need, However for Viking PA, there isn't any such case.

3 Password and Account Settings

3.1 Access Control

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

- **ECR Integrated setup:**

It is not possible to access transaction types such as Refund, Deposit and Reversal from terminal menu to make these functions secure from getting misused. These are the transaction types where money flow occurs from merchant's account to cardholder's account.

- **Standalone setup:**

Merchant card access control is default enabled to access transaction types such as Refund, Deposit and Reversal from terminal menu to make these functions secure from getting misused.

3.2 Password Controls

The Viking payment application does not have user accounts or corresponding passwords; therefore the Viking 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.

4 Logging

4.1 Merchant Applicability

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

4.2 Configure Log Settings

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

4.3 Central Logging

The terminal has a generic log mechanism. The mechanism also includes logging of creation and deletion of SW executables.

SW download activities are logged and can be transferred to Host manually via a menu-choice in the terminal or on request from host flagged in ordinary transaction traffic. If SW download activation fails due to invalid digital signatures on the received files, the incident is logged and transferred to Host automatically and immediately.

4.3.1 Enable trace Logging on terminal

To enable trace logging:

1 Swipe Merchant card.
2 Then in the menu select “9 System menu”.
3 Then go to menu “2 System Log”.
4 Type in the technician code, which you can get by phoning Nets MS support.
5 Select “8 Parameters”.
6 Then enable “Logging” to “Yes”.

4.3.2 Send trace Logs to host

To send trace logs:

1 Press Menu key on the terminal and then Swipe Merchant card.
2 Then in the main menu select “7 Operator menu”.
3 Then select “5 Send TraceLogs” to send trace logs to host.

5 Secure Payment Application

5.1 Application SW

The Viking Telium2 terminal application does not use any external SW and HW not belonging to the Viking 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, GPRS, Bluetooth, Wi-Fi, or the PC-LAN running the POS application.

Viking terminal manage all the communication using link layer component. This component is an application loaded in the terminal. The Link Layer can manage several communications at the same time using different peripherals (modem and serial port for example).

It currently supports the following protocols:

- Physical: RS232, internal modem, external modem (via RS232), USB, Ethernet, Wifi, Bluetooth, GSM, GPRS and 3G.
- Data Link: SDLC, PPP.
- Network: IP.
- Transport: TCP.

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.

When integrated with a POS application on a PC, the terminal can be set up to communicate via the PC-LAN running the POS application using either RS232, USB or Bluetooth. Still all functionality of the payment application is running in the terminal SW.

The application protocol (and applied encryption) is transparent and independent of the type of communication.

5.1.1 Payment Host communication TCP/IP parameter setup

Terminal Profile	NORWAY (.no)	SWEDEN (.se)	DENMARK (.dk)	FINLAND (.fi)	GERMANY (.de)	HUNGARY (.hu)	ESTONIAN (.et)	POLISH (.pl)	Netherlands (.nl)	FRANCE (.fr)
Host IP address	**91.102.24.142**									
Communication TCP-IP PORT	9670	9682	9680	9681	9684	9685	9686	9683	9687	9688

5.1.2 ECR communication

- RS232 Serial
- USB Connection
- TCP/IP parameter setup, also known as ECR over IP

Terminal Profile	NORWAY (.no)	SWEDEN (.se)	DENMARK (.dk)	FINLAND (.fi)	GERMANY (.de)	HUNGARY (.hu)	ESTONIAN (.et)	POLISH (.pl)	Netherlands (.nl)
ECR IP address	Set ECR IP address								
Communication TCP-IP PORT	6001								

5.1.3 Communication to host via ECR

Host IP address	**91.102.24.142**
Communication TCP-IP PORT	9670

5.2 Supported terminal hardwares

Viking PA is supported on variety of PTS (PIN transaction security) validated Ingenico devices. The list of terminal hardware along with their PTS approval number is given below.

Terminal hardware	PTS version	PTS approval number
iPP350	3.x	4-20184
iPP350	4.x	4-30176
iWL250G, IWL250B, IWL255 (3G)	3.x	4-20181
ICT220, ICT250	3.x	4-20196
iUP250 PTS 3.0 + iUR250	3.x	4-30075, 4-30083
iUC180B + iUR250	3.x	4-30100, 4-30083
iCMP (iCM122)	3.x	4-20235
iSMP Companion (iMP3 Companion)	3.x	4-20183
iUP250LE + iUR250 + iUC150B	4.x	4-30251, 4-30250, 4-30172
IMP 627 , IMP 657 (ISMP 4 COMPANION)	4.x	4-30220
IMP 550 (ISMP 3 Sleeve)	4.x	4-30175

6 Wireless Networks

6.1 Merchant Applicability

Viking does not make use of wireless technology. However, the use of wireless is possible together with Viking, in order for Wireless to be implemented securely, consideration should be taken when installing and configuring the wireless network as detailed below.

6.2 Recommended Wireless Configurations

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

7 Network Segmentation

7.1 Merchant Applicability

The Viking 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.

8 Secure Remote Software Updates

8.1 Merchant Applicability

Nets securely deliver remote payment applications updates. 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 high-speed 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.
- Nets contact our cashier and / or customer and agree to an update schedule with email, when release note and payment applications updates available. Customers can also view the latest updates, instructions, and the Implement Guide online here.

8.2 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.

8.3 Personal Firewall

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.

8.4 Remote Update Procedures

There are two ways to trigger the terminal to contact the Nets software centre: Either manually via a menu choice in the terminal (swipe merchant card, select menu 8 “Software”, 1 “Fetch software”), or Host initiated. Using the Host initiated method; the terminal automatically receives a command from the Host after it has performed a financial transaction. The command tells the terminal to contact the Nets software centre to check for updates.

9 Remote Access

9.1 Merchant Applicability

Viking 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.

9.2 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.

10 Transmission of Cardholder Data

10.1 Transmission of Cardholder Data

Viking secures cardholder data in transit by using message-level encryption using 3DES-DUKPT (112 bits) for all transmission (including public networks). Security Protocols for IP communications from the PA-DSS Viking application to the Host is not required since message-level encryption is implemented using 3DES-DUKPT (112-bits) as described above. This encryption scheme ensures that even if transactions are intercepted they cannot be modified or compromised in any way as long as 3DES-DUKPT (112-bits) remains considered as strong encryption. As per the DUKPT key management scheme, the 3DES key used is unique to each transaction.

.

10.2 Email and Cardholder Data

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

10.3 Non-Console Administrative Access

Viking does not support Non-Console administrative access. However, for the merchants general knowledge, Non-Console 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.

11 Viking Versioning Methodology and PA-DSS Impact

The Nets versioning methodology consists of a three-part SW version number: n.m.x.
The Viking SW version number is shown like this on the terminal screen when the terminal is powered up: 0nmx

· An update from e.g. 4.1.1 to 4.1.2 is a non-significant functional update. It may not include changes with impact on security or PA-DSS requirements.

· An update from e.g. 4.1.x to 4.2.x is a non-significant functional update. It may include changes with impact on security or PA-DSS requirements.
· An update from e.g. 5.0.x to 6.0.x is a significant functional update. It may include changes with impact on security or PA-DSS 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.

12 Instructions about secure installation of patches and updates.

NETS securely deliver remote payment applications updates.
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 high-speed connections, updates are received through a firewall or personel firewall.

The Nets host is available either via internet using secure access or via a closed network. With closed network the network provider has a direct connection to our host environment offered from their network provider.
The terminals are managed through Nets terminal management services. The terminal management service defines for example the region the terminal belongs to and the acquirer in use.
Terminal management is also responsible for upgrading terminal software remotely over the network. Nets ensure that the software uploaded to the terminal has completed the required certifications.

NETS recommends check points to all its customers to ensure safe and secure payments as listed below:

1. Keep a list of all operational payment terminals and take pictures from all dimensions so you know what they are supposed to look like.
2. Look for obvious signs of tampering such as broken seals over access cover plates or screws, odd or different cabling or a new hardware device that you can't recognize.
3. Protect your terminals from customer's reach when not in use. Inspect your payment terminals on daily basis and other devices which can read payment cards.
4. You must check identity of repair personnel if you are expecting any payment terminal repairs.
5. Call NETS or your bank immediately if you suspect any unobvious activity.
6. If you believe that your POS device is vulnerable to theft then there are service cradles and secure harnesses and tethers available to purchase commercially. It may be worth considering their use.

13 PA-DSS Requirements Reference

Chapter in this document	PA-DSS Requirements Reference	PCI DSS requirements
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	3.2 3.2 3.1 3.3 3.4 3.5 3.6 3.6
Chapter 3 : Password and Account Settings	3.1 3.2	8.1 & 8.2 8.1 & 8.2
Chapter 4 : Logging	4.1 4.4	10.1 10.5.3
Chapter 5 : Secure Payment Application	8.2	2.2.3
Chapter 6 : Wireless Network	6.1 6.2 6.3	1.2.3 & 2.1.1 4.1.1 1.2.3, 2.1.1,4.1.1
Chapter 7 : Network Segmentation	9.1	1.3.7
Chapter 8 : Secure Remote Software Updates	10.2.1 10.2.3	1&12.3.9 2, 8, & 10
Chapter 9 : Remote Access	10.1	8.3
Chapter 10 : Transmission of Cardholder Data	11.1 11.2 12.1 12.2	4.1 4.2 2.3 8.3
Chapter 11: Viking Versioning Methodology and PA-DSS Impact	5.4.4	
Chapter 12: Provide instructions for customers about secure installation of patches and updates.	7.2.3	

14 Glossary of Terms

TERM	DEFINITION
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.
Merchant	The end user and purchaser of the Viking product.
PA-DSS	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)
PA-QSA	Payment Application Qualified Security Assessors. QSA company that provides services to payment application vendors in order to validate vendors' payment applications.
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.
Viking	The software platform used by Nets for application development for the European market.

15 Document Control

Document Information

Document Reference:	Viking Implementation Guide Telium
Document Location:	Undisclosed

Document Author, Reviewers and Approvers

Description	Function	Name
PA-QSA	Reviewer	Claudio Adami
QA	Reviewer & Approver	Varun Shukla
Compliance	Author	Seija Salo
Compliance Manager	Reviewer & Approver	Ove Skeie
Development	Reviewer & Approver	Navneet Chhabra
Product Manager	Reviewer & Approver	May-Britt Denstad Sandersnäs
Project Manager	Reviewer & Approver	Henri Korhonen
Delivery/Department Manager	Manager	Ossi Korhonen

Summary of Changes

Version Number	Version Date	Nature of Change	Change Author	Revision Tag	Date Approved
1.0	01.07.2010	Complete Revision	Ole Kjøsterud		01.07.2010
1.1	22.12.2010	All document updated after merged between PBS, BBS and Teller. Change BBS AS to NETS AS. 10. Glossary of Term: - Added new term. - Updated definition of Viking.	Carla Sandbakken		22.12.2010
1.2	17.02.2012	Updated after PA-DSS assessment for Viking 3.2, based on PA-DSS version 2.0. - Added point 2.6 'Key Management' - Added new chapters: Chapter 5: Secure Payment Application. Chapter 11: PA-DSS Reference - Updated chapter title 'Encrypting Network Traffic' to 'Transmission of Cardholder Data'	Svanhild Gundersen		17.12.2010
1.3	09.07.2012	Updated after PA-DSS assessment for Viking 3.3 which is PA-DSS minor change with regard to Viking 3.2. There is no change in the content of the document other than the software version reference which is changed from 3.2 to 3.3.	Kevin Rodrigues		09.07.2012
1.3	09.08.2012	No change in content, version updated to 3.4	Vegar Kjekshus		09.08.2012
1.4	05.10.2012	No change in content, Telium version updated to 3.6.	Ole Kjøsterud		05.10.2012
1.5	12.03.2013	Updated the name of Delivery Manager.	Ilona Sondore		12.03.2013
1.6	25.04.2013	Updated chapter 6.2 Recommended Wireless Configurations. Described more in details and added: Change any other security defaults provided or set by the vendor	Ilona Sondore		25.04.2013
1.7	23.05.2013	No change in content, Telium version updated to 3.8.	Ilona Sondore		23.05.2013
1.8	12.08.2013	Changed document name	Ilona Sondore		12.08.2013

1.9	02.09.2013	Corrected a few misspellings in document, Telium version updated to 4.0	Svanhild Gundersen	02.09.2013
2.0	27.01.2014	Added a chapter on version methodology and Release history. Updated the name of Delivery Manager.	Svanhild Gundersen	05.02.2014
2.1	14.05.2014	Updated Release History and name of Delivery Manager	Svanhild Gundersen	14.05.2014
2.2	24.09.2014	Changes on company name from “Nets Terminal Norway” to “Nets Norway AS”.	Ilona Sondore	24.09.2014
2.3	05.10.2014	Updated release history Changed NETS to Nets. Removed SSL as a secure communication protocol from sections 9.2 and 10.3	Svanhild Gundersen	17.10.2014 22.12.2014
2.4	26.01.2015	Updated to be compliant with PA-DSS version 3; updated SW versioning methodology and Release History; updated PA-DSS requirement reference	Svanhild Gundersen	03.02.2015
2.5	23.06.2015	Release history updated	Svanhild Gundersen	23.06.2015
2.6	27.08.2015	Changed the company name from “Nets NORWAY AS” to “Nets Branch Norway”. Updated name of Delivery Manager and Development	Mikko Kohonen	28.08.2015
2.7	31.08.2015	Release history updated	Mikko Kohonen	02.09.2015
2.8	18.11.2015	Release history updated. Document Author, Reviewers and Approvers updated.	Mikko Kohonen	28.08.2015
2.9	22.02.2016	Changed the company name from “Nets Branch Norway ” to “Nets Oy”.	Seija Salo	22.02.2016
3.0	23.2.2016	Release history updated.	Seija Salo	23.2.2016
3.1	29.02.2016	Updated Delivery Manager name	Shamsher Singh	29.02.2016
3.2	08.07.2016	Release history updated	Seija Salo	08.07.2016
3.3	14.10.2016	Release history updated	Seija Salo	17.10.2016
3.4	22-11-2016	Release history updated	Mayuresh Sawant	12.12.2016
3.5	20.01.2017	Updated PADSS approval reference	Seija Salo	20.01.2017
3.6	24.04.2017	Added PCI DSS requirement/	Seija Salo/Navneet	25.04.2017
3.7	26.06.2017	Added Padss ref. number	Seija Salo	16.06.2017
3.8	16.11.2017	Added chapter 12 (Instruction for customer about secure installations) Also updated chapter 13 PA-DSS requirements reference	Navneet	21.11.2017
3.9	26.01.2018	Added 5.1 version Padss ref. number	Seija Salo	26.01.2018
4.0	27.04.2018	Updated section 2.1 Merchant Applicability	Navneet	27.04.2018
4.1	08.06.2018	Updated section 5.1 and 5.2 Software and hardware components	Navneet	08.06.2018
4.2	23.07.2018	Updated section 11 Viking versioning methodology, removed software components table, added TCP-IP parameters for host and ECR integration from section 5.1 Updated section 15 Author, reviewer list.	Navneet	10.01.2019
4.3	04.09.2019	Updated Sections 2.5, 4.3 and 10.1	Shamsher	04.09.2019
4.4	13.09.2019	Updated section 5.1.1 and SW version number	Seija	13.09.2019
4.5	01.10.2019	PA QSA review updated, PADSS version typo fixed	Seija	01.10.2019
4.6	02.10.2019	Updated section 5.1.1, SW version number , PA QSA and Project Manager updated	Seija	02.10.2019

Distribution List

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

Document Approvals

Name	Function
Henri Korhonen	Delivery Manager

Document Review Plans

This document will be reviewed and updated, if necessary as defined below:

- As required to correct or enhance information content
- Following any organizational changes or restructuring
- Following an annual review
- Following exploitation of a vulnerability
- Following new information / requirements regarding relevant vulnerabilities