Nets Branch Norway:
PA-DSS Implementation Guide for Viking 4.4.x

Version 2.5

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 3.0
- PCI DSS version 3.0

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 not retain cardholder data and 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. When the key space is exhausted, the terminal has to be replaced.

3 Password and Account Settings

3.1 Access Control

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

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.

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, or the PC-LAN running the POS application.

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.

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.

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

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: nn.m.x.
The Viking SW version number is shown like this on the terminal screen when the terminal is powered up: nnmx

· 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. 4.1.x to 5.0.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.

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**
3.2	12-08.00424.003	Full validation	
3.3	12-08.00424.003.aaa	No-Impact	
3.4	12-08.00424.005	Full Validation	
3.6	12-08.00424.006	Full Validation	
3.7	12-08.00424.006.aaa	High-Impact	Adding of unattended terminal model iUP250 with reader IUR250.
3.8	12-08.00424.006.baa	High-Impact	Adding of contactless reader iUC150 to the unattended terminal. Adding the possibility of non-PIN transactions for unattended terminals. It is intended for amounts below 50€ in parking environments.
3.9	12-08.00424.006.caa	Low-Impact	

4.0	12-08.00424.006.daa	High-Impact	Added support to send non-branded card info to ECR using whitelist to identify the cards.
4.1	12-08.00424.006.eaa	High-Impact	Adding of new terminal models: iUC180B, iWL255G and iCMP.
4.2	12-08.00424.006.faa	High-impact	Adding of new terminal model iSMP companion (iMP3 companion)
4.3	12-08.00424.006.gaa	High-impact	Choosing BAX in a multiterminal configuration based on truncated PAN received from card.
4.4.x	15-08.00424.007	Full validation	Compliance with PA-DSS v3.

12 PA-DSS Requirements Reference

Chapter in this document	PA-DSS Requirements Reference
Chapter 2 : Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data	1.1.4 1.1.5 2.1 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 Segmentation	9.1
Chapter 8 : Secure Remote Software Updates	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: Viking Versioning Methodology	5.4.4

13 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.

14 Document Control

Document Information

Document Reference:	Viking Implementation Guide Telium
Document Location:	Undisclosed

Document Author, Reviewers and Approvers

Description	Function	Name
PA-QSA	Author	Johan Hagdahl
QA	Reviewer & Approver	Mona Boldermo
Compliance	Reviewer & Approver	Arild Enevoldsen
Development	Reviewer & Approver	Svanhild Gundersen
Project Manager	Reviewer & Approver	Carla Sandbakken
Delivery Manager	Reviewer	Jon Steinar Jensen

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 methodol-	Svanhild		05.02.2014

		ogy and Release history. Updated the name of Delivery Manager.	Gundersen	
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	23.07.2015	Changed the company name from “Nets Norway AS” to “Nets Branch Norway”.	Shamsher Singh	23.07.2015

Distribution List

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

Document Approvals

Name	Function
Jon Steinar Jensen	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