Nets Denmark A/S:
PCI-Secure Software Standard
Software Vendor Implementation Guide
for Viking terminal 1.02.0

Version 1.2

Contents

1. Introduction and Scope 4
1.1 Introduction 4
1.2 Software Security Framework (SSF) 4
1.3 Software Vendor Implementation Guide - Distribution and Updates 4

2. Secure Payment Application 5
2.1 Application S/W 5
2.1.1 Payment Host communication TCP/IP parameter setup 5
2.1.2 ECR communication 6
2.1.3 Communication to host via ECR 6
2.2 Supported terminal hardware(s) 7
2.3 Security Policies 9

3. Secure Remote Software Update 10
3.1 Merchant Applicability 10
3.2 Acceptable Use Policy 10
3.3 Personal Firewall 10
3.4 Remote Update Procedures 10

4. Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data 11
4.1 Merchant Applicability 11
4.2 Secure Delete Instructions 11
4.3 Locations of Stored Cardholder Data 11
4.4 Deferred Authorization Transaction 12
4.5 Troubleshooting Procedures 12
4.6 PAN locations - Displayed or Printed 12
4.7 Prompt files 13
4.8 Key management 13
4.9 '24 HR' Reboot 14
4.10 Whitelisting 14

5. Authentication and Access Controls 15
5.1 Access Control 15
5.2 Password Controls 17

6. Logging 18
6.1 Merchant Applicability 18
6.2 Configure Log Settings 18
6.3 Central Logging 18
6.3.1 Enable trace Logging on terminal 18
6.3.2 Send trace Logs to host 18
6.3.3 Remote trace logging 18
6.3.4 Remote error logging 19

7. Wireless Networks 20
7.1 Merchant Applicability 20
7.2 Recommended Wireless Configurations 20

8. Network Segmentation 21
8.1 Merchant Applicability 21

9. Remote Access 22
9.1 Merchant Applicability 22

10. Transmission of Sensitive data 23
10.1 Transmission of Sensitive data 23
10.2 Sharing Sensitive data to other software 23
10.3 Email and Sensitive data 23
10.4 Non-Console Administrative Access 23

11. Viking Versioning Methodology 24

12. Instructions about Secure Installation of Patches and Updates. 25

13. Viking Release Updates 26

14. Not-Applicable requirements 27

15. PCI Secure Software Standard Requirements Reference 31

16. Glossary of Terms 32

17. Document Control 33

1. Introduction and Scope

1.1 Introduction

The purpose of this PCI-Secure Software Standard Software Vendor Implementation Guide is to provide stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of the Viking software. The guide instructs Merchants on how to implement Nets' Viking application into their environment in a PCI Secure Software Standard compliant manner. Although, it is not intended to be a complete installation guide. Viking application, if installed according to the guidelines documented here, should facilitate, and support a merchant's PCI compliance.

1.2 Software Security Framework (SSF)

The PCI Software Security Framework (SSF) is a collection of standards and programs for the secure design and development of payment application software. The SSF replaces the Payment Application Data Security Standard (PA-DSS) with modern requirements that support a broader array of payment software types, technologies, and development methodologies. It provides vendors with security standards like PCI Secure Software Standard for developing and maintaining payment software so that it protects payment transactions and data, minimizes vulnerabilities, and defends against attacks.

1.3 Software Vendor Implementation Guide - Distribution and Updates

This PCI Secure Software Standard Software Vendor 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 Secure Software Standard.

Nets publishes information on the listed website if there are any updates in the implementation guide.

Website: https://support.nets.eu/

For Example: Nets PCI-Secure Software Standard Software Vendor Implementation Guide will be distributed to all customers, resellers, and integrators. Customers, Resellers, and Integrators will be notified from reviews and updates.

Updates to the PCI-Secure Software Standard Software Vendor Implementation Guide can be obtained by contacting Nets directly, as well.

This PCI-Secure Software Standard Software Vendor Implementation Guide references both the PCI-Secure Software Standard and PCI requirements. The following versions were referenced in this guide.

- PCI-Secure-Software-Standard-v1_1

2. Secure Payment Application

2.1 Application S/W

The Viking payment applications do not use any external software or hardware not belonging to the Viking embedded application. All S/W executables belonging to the Viking payment application are digitally signed with Tetra signing kit provided by Ingenico.

- The terminal communicates with the Nets Host using TCP/IP, either via Ethernet, GPRS, Wi-Fi, or via the PC-LAN running the POS application. Also, the terminal can communicate with the host via mobile with Wi-Fi or GPRS connectivity.

Viking terminals manage all the communication using Ingenico 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, Wi-Fi, Bluetooth, GSM, GPRS, 3G and 4G.
- 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 S/W in the terminal, and the terminal S/W 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 RS232, USB, or Bluetooth. Still all functionality of the payment application is running in the terminal S/W.

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

2.1.1 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)	SPAIN (.sp)	UNITED KINGDOM (.uk)	LATVIAN (.lv)	LITHUANIAN (.lt)
Host IP address	91.102.24.142													
Communication TCP-IP PORT	9670	9682	9680	9681	9684	9685	9686	9683	9687	9688	9689	9679	9690	9691

2.1.2 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)	NETHER LANDS (.nl)	FRANCE (.fr)	SPAIN (.sp)	UNITED KINGDOM (.uk)	LATVIAN (.lv)	LITHUANIAN (.lt)
ECR IP address	Set ECR IP address													
Communication TCP-IP PORT	6001													

- Host/ECR communication options in Viking Payment Application

Host Comm Type	Terminal Type
Ethernet	Self4000, Move3500, Desk3500, Lane3000
BT iOS	Link2500, Link2500i
BT Android	Move3500, Link2500, Link2500i
via ECR	Self4000, Move3500, Link2500, Link2500i, Desk3500, Lane3000
GPRS	Move3500
Wifi	Move3500, Link2500

ECR Comm Type	Terminal Type
IP Ethernet	Self4000, Move3500, Desk3500, Lane3000
BT iOS	Link2500, Link2500i
BT Android	Move3500, Link2500, Link2500i
USB	Self4000, Move3500, Link2500, Link2500i, Desk3500, Lane3000
RS232	Self4000, Desk3500, Lane3000
GPRS	Move3500
IP Wifi	Move3500, Link2500

- Nets Cloud ECR (Connect@Cloud) parameters configuration

ECR IP address	212.226.157.243
Communication TCP-IP PORT	6001

2.1.3 Communication to host via ECR

Host IP address	91.102.24.142
Communication TCP-IP PORT (NORWAY)	9670

Note: Refer "2.1.1- Payment Host communication TCP/IP parameter setup" for country specific TCP/IP ports.

2.2 Supported terminal hardware(s)

Viking payment application 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.

Tetra Terminal Types

Terminal hardware	PTS version	PTS approval number	PTS Hardware Version	PTS Firmware Version
Lane 3000	5.x	4-30310	LAN30AN LAN30BA LAN30BN LAN30CA LAN30DA LAN30EA LAN30EN LAN30FA LAN30FN LAN30GA LAN30HA LAN30AA	820547v01.xx 820561v01.xx
Desk 3500	5.x	4-20321	DES32BB DES32BC DES32CB DES32DB DES32DC DES35AB DES35BB DES35BC DES35CB DES35DB DES35DC DES32AB	820376v01.xx 820376v02.xx 820549v01.xx 820555v01.xx 820556v01.xx 820565v01.xx 820547v01.xx
Move 3500	5.x	4-20320	MOV35AC MOV35AQ MOV35BB MOV35BC MOV35BQ MOV35CB MOV35CC MOV35CQ MOV35DB MOV35DC MOV35DQ MOV35EB MOV35FB MOV35JB MOV35AB	820376v01.xx 820376v02.xx 820547v01.xx 820549v01.xx 820555v01.xx 820556v01.xx 820565v01.xx 820547v01.xx 820565v01.xx
Link2500	4.x	4-30230	LIN25BA LIN25BB LIN25CA LIN25DA LIN25DB LIN25EA LIN25FA	820555v01.xx 820556v01.xx 820547v01.xx

			LIN25FB LIN25GA LIN25HA LIN25HB LIN25IA LIN25JA LIN25JB LIN25KA LIN25LA LIN25MA LIN25NA LIN25AA	
Link2500	5.x	4-30326	LIN25BA LIN25BB LIN25CA LIN25DA LIN25DB LIN25EA LIN25FA LIN25FB LIN25GA LIN25HA LIN25HB LIN25IA LIN25JA LIN25JB LIN25KA LIN25LA LIN25MA LIN25NA LIN25AA LIN25BB	820547v01.xx
Self4000	5.x	4-30393	SEL40BA	820547v01.xx

2.3 Security Policies

Viking payment application adheres to all the applicable security policies specified by Ingenico. For general information, these are the links to the security policies for different Tetra terminals:

Terminal Type	Security Policy document
Link2500 (v4)	Link/2500 PCI PTS Security Policy (pcisecuritystandards.org)
Link2500 (v5)	PCI PTS Security Policy (pcisecuritystandards.org)
Desk3500	https://listings.pcisecuritystandards.org/ptsdocs/4-20321ICO-OPE-04972-EN-V12_PCI_PTS_Security_Policy_Desk_3200_Desk_3500-1650663092.33407.pdf
Move3500	https://listings.pcisecuritystandards.org/ptsdocs/4-20320ICO-OPE-04848-EN-V11_PCI_PTS_Security_Policy_Move_3500-1647635765.37606.pdf
Lane3000	https://listings.pcisecuritystandards.org/ptsdocs/4-30310SP_ICO-OPE-04818-EN-V16_PCI_PTS_Security_Policy_Lane_3000-1648830172.34526.pdf
Self4000	Self/4000 PCI PTS Security Policy (pcisecuritystandards.org)

3. Secure Remote Software Update

3.1 Merchant Applicability

Nets securely delivers Viking payment application updates remotely. 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.

3.2 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.

3.3 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.

3.4 Remote Update Procedures

There are two ways to trigger the terminal to contact the Nets software center for updates:

1. Either manually via a menu option in the terminal (swipe merchant card, select menu 8 “Software”, 1 “Fetch software”), or Host initiated.
2. 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.

After a successful software update, a terminal with a built-in printer will print a receipt with information on the new version.

Terminal integrators, partners and/or Nets technical support team 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, Viking payment application can be also validated via Terminal Info on pressing ‘F3’ key on the terminal.

4. Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data

4.1 Merchant Applicability

Viking payment application does not store any magnetic stripe data, card validation values or codes, PINs or PIN block data, cryptographic key material, or cryptograms from its previous versions.

To be PCI compliant, a merchant must have a data-retention policy which defines how long cardholder data will be kept. Viking payment application does retain cardholder data and/or sensitive authentication data of the very last transaction and in case if there are offline or deferred authorization transactions while adhering to the PCI-Secure Software Standard compliance at the same time, hence it can be exempt from the merchant's cardholder data-retention policy.

4.2 Secure Delete Instructions

The terminal does not store sensitive authentication data; full track2, CVC, CVV or PIN, neither before nor after authorization; except for Deferred Authorization transactions in which case encrypted sensitive authentication data (full track2 data) is stored until authorization is done. Post authorization the data is deleted securely.

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.

4.3 Locations of Stored Cardholder Data

Cardholder data is stored in the Flash DFS (Data File System) of the terminal. The data is not directly accessible by the merchant.

Data Store (file, table, etc.)	**Cardholder Data Elements stored** (PAN, expiry, any elements of SAD)	**How data store is secured** (for example, encryption, access controls, truncation, etc.)
File: trans.rsd	PAN, Expiry Date, Service Code	PAN: Encrypted 3DES-DUKPT (112 bits)
File: storefwd.rsd	PAN, Expiry Date, Service Code	PAN: Encrypted 3DES-DUKPT (112 bits)
File: transoff.rsd	PAN, Expiry Date, Service Code	PAN: Encrypted 3DES-DUKPT (112 bits)
File: transorr.rsd	Truncated PAN	Truncated (First 6, Last 4)
File: offlrep.dat	Truncated PAN	Truncated (First 6, Last 4)
File: defauth.rsd	PAN, Expiry Date, Service Code	PAN: Encrypted 3DES-DUKPT (112 bits)
File: defauth.rsd	Full track2 data	Full Track2 data: pre-Encrypted 3DES-DUKPT (112 bits)

4.4 Deferred Authorization Transaction

Deferred Authorization occurs when a merchant cannot complete an authorization at the time of the transaction with the cardholder due to connectivity, systems issues, or other limitations, and then later completes the authorization when it is able to do so.

That means that a deferred authorization occurs when an online authorization is performed after the card is no longer available. As the online authorization of deferred authorization transactions are delayed, the transactions will be stored on terminal until the transactions are successfully authorized later when network is available.

The transactions are stored and sent later to the host, like how the Offline transactions are stored as of today in Viking payment application.

Merchant can initiate the transaction as 'Deferred Authorization' from the Electronic Cash Register (ECR) or via terminal menu.

Deferred Authorization transactions can be uploaded to the Nets host by merchant using below options:

1. ECR - Admin command - Send offline (0x3138)
2. Terminal - Merchant ->2 EOT -> 2 sent to host

4.5 Troubleshooting Procedures

Nets support will not request sensitive authentication or cardholder data for troubleshooting purposes. Viking payment application is not capable of collecting or troubleshooting the sensitive data in any case.

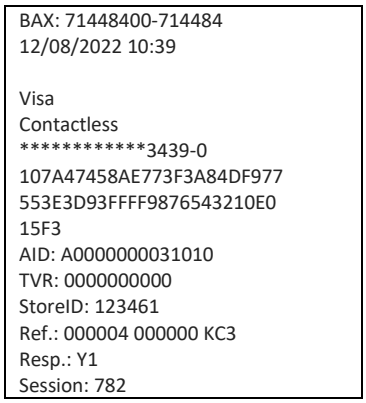
4.6 PAN locations - Displayed or Printed

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 with * where first 6 digits and last 4 digits are in clear text.
- Transaction list report:
  Transaction list report shows the transactions performed in a session. Transaction details include Masked PAN, Card issuer name and the transaction amount.
- Last customer receipt:
  The copy of last customer receipt can be generated from terminal copy 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 112-bit DUKPT encrypted cardholder data (PAN, Expiry date and Service code).



PURCHASE
NOK 12,00

APPROVED

RETAILER COPY

Confirmation:

Viking payment application 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 payment application 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 payment application, there isn't any such case.

Example for masked PAN:

PAN: 957852181428133823-2

Minimum info: **********3823-2

Maximum info: 957852********3823-2

4.7 Prompt files

Viking payment application do not provide any separate prompt files.

Viking payment application requests for cardholder inputs through display prompts which are part of the messaging system within the signed Viking payment application.

Display prompts for PIN, amount, etc. are shown on the terminal, and cardholder inputs are awaited. The inputs received from cardholder are not stored.

4.8 Key management

For the Tetra range of terminal models, all security functionality is performed in a secure area of a PTS device 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. All key exchange between Nets host, Key/Inject tool (for Tetra terminals) and the PED are done in encrypted form.

Procedures for Key Management are implemented by Nets according to a DUKPT scheme using 3DES encryption.

All keys and key components used by Nets terminals are generated using approved random or pseudorandom processes. Keys and key components used by Nets terminals are generated by Nets key management system, which use approved Thales Payshield HSM units to generate cryptographic keys.

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, and then the terminal must be replaced.

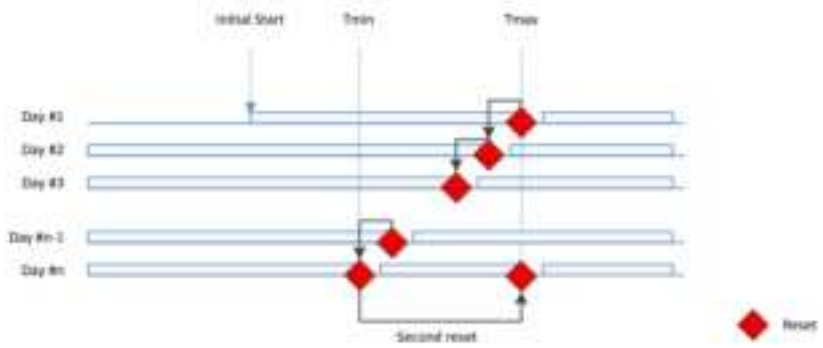
4.9 ‘24 HR’ Reboot

All Viking terminals are PCI-PTS 4.x and above and hence follows the compliance requirement that PCI-PTS 4.x terminal shall reboot minimum once every 24 hours to wipe the RAM and further secure terminal HW from being used to get hold of payment card data.

Another benefit of the ‘24hr’ re-boot cycle is that memory leaks will be mitigated and have less impact for the merchant (not that we should accept memory leak issues.

Merchant can set the reboot time from the terminal Menu option to ‘Reboot Time’. The reboot time is set based on ‘24hr’ clock and will take the format HH:MM.

The Reset mechanism is designed to ensure a terminal reset at least one time per 24 hours running. To fulfil this requirement a time slot, called the “reset interval” represented by Tmin and Tmax has been defined. This period represents the time interval where the reset is allowed. Depending on the business case, the “reset interval” is customized during the terminal installation phase. By design, this period cannot be shorter than 30 minutes. During this period, the reset occurs each day 5 minutes earlier (on T3) as explained by the diagram below:



4.10 Whitelisting

Whitelisting is a procedure to determine that the PANs listed as a whitelist are allowed to be shown in clear text. Viking uses 3 fields for determining the whitelisted PANs which are read from the configurations downloaded from the terminal management system.

When a ‘Compliance flag' in Nets host is set to Y, the information from the Nets Host or Terminal management system is downloaded to the terminal, when the terminal starts. This Compliance flag is being used for determining the whitelisted PANs which are read from the dataset.

‘Track2ECR’ flag determines whether the Track2 data is allowed to be handled(sent/received) by the ECR for a specified issuer. Depending on the value of this flag, it is determined if the track2 data should be shown in local mode on ECR.

‘Print format field’ determines how the PAN will be displayed. The cards in PCI scope will all have the print format set to display the PAN in truncated/masked form.

5. Authentication and Access Controls

5.1 Access Control

The Viking payment application does not have user accounts or corresponding passwords therefore, the Viking payment application is exempt from this requirement.

- **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. It is the merchant's responsibility to ensure that ECR is used only by authorized users.

- **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.

The Viking terminal is configured by default to secure the menu options, to prevent unauthorized access. The parameters to configure the menu security falls under Merchant Menu (accessible with a Merchant card) -> Parameters -> Security

Protect menu – Set to 'Yes' by default.

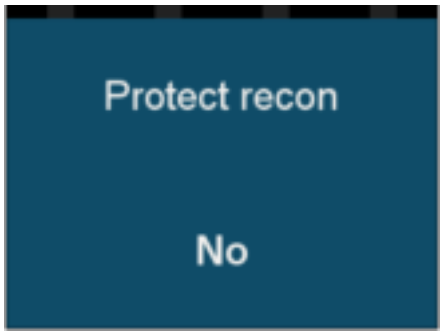
Menu button on the terminal is protected using the Protect menu configuration. Menu can be accessed only by the Merchant using a merchant card.

Protect reversal – Set to 'Yes' by default.

Reversal of a transaction can only be done by the merchant using the merchant card to access the reversal menu.

Protect reconciliation – Set to 'Yes' by default

Option for Reconciliation can be accessed only by the merchant with the merchant card when this protection is set to true.



Protect Shortcut – Set to 'Yes' by default

Shortcut menu with the options for viewing Terminal Info and option for updating Bluetooth parameters will be available to the merchant only when merchant card is swiped.

5.2 Password Controls

The Viking payment application does not have user accounts or corresponding passwords; therefore, the Viking application is exempt from this requirement.

6. Logging

6.1 Merchant Applicability

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

6.2 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 payment application does not log any sensitive authentication data or cardholder data.

6.3 Central Logging

The terminal has a generic log mechanism. The mechanism also includes logging of creation and deletion of S/W executable.

S/W 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 S/W download activation fails due to invalid digital signatures on the received files, the incident is logged and transferred to Host automatically and immediately.

6.3.1 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 calling Nets Merchant Service support.
5 Select “8 Parameters”.
6 Then enable “Logging” to “Yes”.

6.3.2 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 Trace Logs” to send trace logs to host.

6.3.3 Remote trace logging

A parameter is set in the Nets Host (PSP) which will enable/disable Terminal’s trace logging functionality remotely. Nets Host will send Trace enable/disable logging parameter to Terminal in Data set along with the scheduled time when Terminal will upload Trace logs. When terminal receives Trace parameter as enabled, it would start capturing Trace logs and at the scheduled time it will upload all trace logs and disable the logging functionality thereafter.

6.3.4 Remote error logging

Error logs are always enabled on the terminal. Like trace logging, a parameter is set in the Nets Host which will enable/disable Terminal's error logging functionality remotely. Nets Host will send Trace enable/disable logging parameter to Terminal in Data set along with the scheduled time when Terminal will upload Error logs. When terminal receives Error logging parameter as enabled, it would start capturing Error logs and at the scheduled time it will upload all error logs and disable the logging functionality thereafter.

7. Wireless Networks

7.1 Merchant Applicability

Viking payment terminal - MOVE 3500 and Link2500 have the capability to connect with Wi-Fi network. Therefore, for Wireless to be implemented securely, consideration should be taken when installing and configuring the wireless network as detailed below.

7.2 Recommended Wireless Configurations

There are many 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 are 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

8. Network Segmentation

8.1 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 demilitarized zone (DMZ) must be set up to segment the network so that only machines on the DMZ are Internet accessible.

9. Remote Access

9.1 Merchant Applicability

Viking payment application 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.

10. Transmission of Sensitive data

10.1 Transmission of Sensitive data

Viking payment application secures sensitive data and/or 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 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 if 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 Sharing Sensitive data to other software

The Viking payment application does not provide any logical interface(s)/APIs to enable the sharing of cleartext account data directly with other software. No sensitive data or cleartext account data is shared with other software through exposed APIs.

10.3 Email and Sensitive data

Viking payment application does not natively support the sending of email.

10.4 Non-Console Administrative Access

Viking does not support non-Console administrative access.

However, for the merchant's 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

The Nets versioning methodology consists of a three-part S/W version number: a.bb.c

where ‘a’ will be incremented when high impact changes are done as per PCI-Secure Software Standard.
a - major version (1 digit)

‘bb’ will be incremented when low impact planned changes are done as per PCI-Secure Software Standard.
bb - minor version (2 digits)

'c' will be incremented when low impact patch changes are done as per PCI-Secure Software Standard.
c - minor version (1 digit)

The Viking payment application S/W version number is shown like this on the terminal screen when the terminal is powered up: ‘abbc’

- An update from e.g., 1.00.0 to 2.00.0 is a significant functional update. It may include changes with impact on security or PCI Secure Software Standard requirements.
- An update from e.g., 1.00.0 to 1.01.0 is a non-significant functional update. It may not include changes with impact on security or PCI Secure Software Standard requirements.
- An update from e.g., 1.00.0 to 1.00.1 is a non-significant functional update. It may not include changes with impact on security or PCI Secure Software Standard requirements.

All changes are represented in sequential numeric order.

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.

When there is a patch, Nets will update the patch version on Nets Host. Merchant would get the patches through automated S/W download request, or the merchant can also initiate a software download from the terminal menu.

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 personnel 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 recommend 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. Viking Release Updates

The Viking software is released in the following release cycles (subject to changes):

- 2 major releases annually
- 2 minor releases annually
- Software patches, as and when required, (for e.g. due to any critical bug/vulnerability issue). If a release is operational in field and some critical issue(s) are reported, then a software patch with the fix is expected to be released within one months' time.

Merchants would be notified about the releases (major/minor/patch) through emails that would be directly sent to their respective email addresses. The email will also contain the major highlights of the release and release notes.

The merchants can also access the release notes which will be uploaded at:

Software release notes (nets.eu)

Viking Software releases are signed using Ingenico's singing tool for Tetra terminals. Only signed software can be loaded onto the terminal.

14. Not-Applicable requirements

This section holds a list of requirements in the PCI-Secure Software Standard that has been assessed as 'Not-Applicable' to the Viking payment application and the justification for this.

PCI Secure Software Standard CO	Activity	Justification for being 'Not-applicable'
5.3	Authentication methods (including session credentials) are sufficiently strong and robust to protect authentication credentials from being forged, spoofed, leaked, guessed, or circumvented.	Viking payment application runs on PCI approved PTS POI device. Viking payment application does not offer local, non-console or remote access, nor level of privileges, thus there is no authentication credentials in the PTS POI device. Viking payment application does not provide settings to manage or generate user IDs and does not provide any local, non-console or remote access to critical assets (even for debug purposes).
5.4	By default, all access to critical assets is restricted to only those accounts and ser vices that require such access.	Viking payment application runs on PCI approved PTS POI device. Viking payment application does not provide settings to manage or generate accounts or services.
7.3	All random numbers used by the software are generated using only approved random number generation (RNG) algorithms or libraries. Approved RNG algorithms or libraries are those that meet industry standards for sufficient unpredictability (e.g., NIST Special Publication 800-22).	Viking payment application does not use any RNG (random number generator) for its encryption functions. Viking payment application does not generate nor use any random numbers for cryptographic functions.
7.4	Random values have entropy that meets the minimum effective strength requirements of the cryptographic primitives and keys that rely on them.	Viking payment application does not use any RNG (random number generator) for its encryption functions. Viking payment application does not generate nor use any random numbers for cryptographic functions.
8.1	All access attempts and usage of critical assets is tracked and traceable to a unique individual.	Viking payment application runs on PCI approved PTS POI devices, where all critical asset handling happens, and the PTS POI firmware ensure confidentiality and integrity of sensitive data while stored within the PTS POI device. Viking payment application's sensitive function's confidentiality, integrity and resiliency are protected and provided by the PTS POI firmware. The PTS POI firmware prevents any access to critical assets out of the terminal and relies on anti-tampering features.

		Viking payment application does not offer local, non-console or remote access, nor level of privileges, thus there is no person or other systems with access to critical assets, only Viking payment application is able to handle critical assets
8.2	All activity is captured in sufficient and necessary detail to accurately describe what specific activities were performed, who performed them, the time they were performed, and which critical assets were impacted.	Viking payment application runs on PCI approved PTS POI devices. Viking payment application does not offer local, non-console or remote access, nor level of privileges, thus there is no person or other systems with access to critical assets, only Viking payment application is able to handle critical assets. • Viking payment application does not provide privilege modes of operation. • There are no functions to disable encryption of sensitive data • There are no functions for the decryption of sensitive data • There are no functions for exporting sensitive data to other systems or processes • There are no authentication features supported Security controls and security functionality cannot be disabled nor deleted.
8.3	The software supports secure retention of detailed activity records.	Viking payment application runs on PCI approved PTS POI devices. Viking payment application does not offer local, non-console or remote access, nor level of privileges, thus there is no person or other systems with access to critical assets, only Viking payment application is able to handle critical assets. • Viking payment application does not provide privilege modes of operation. • There are no functions to disable encryption of sensitive data • There are no functions for the decryption of sensitive data • There are no functions for exporting sensitive data to other systems or processes • There are no authentication features supported

		Security controls and security functionality cannot be disabled nor deleted.
8.4	The software handles failures in activity-tracking mechanisms such that the integrity of existing activity records is preserved.	Viking payment application runs on PCI approved PTS POI devices. Viking payment application does not offer local, non-console or remote access, nor level of privileges, thus there is no person or other systems with access to critical assets, only Viking application is able to handle critical assets. • Viking payment application does not provide privilege modes of operation. • There are no functions to disable encryption of sensitive data • There are no functions for the decryption of sensitive data • There are no functions for exporting sensitive data to other systems or processes • There are no authentication features supported • Security controls and security functionality cannot be disabled nor deleted.
B.1.3	The software vendor maintains documentation that describes all configurable options that can affect the security of sensitive data.	Viking payment application runs on PCI approved PTS POI devices. Viking payment application does not provide any of the following to the end users: • configurable option to access to sensitive data • configurable option to modify mechanisms to protect sensitive data • remote access to the application • remote updates of the application • configurable option to modify default settings of the application
B.2.4	The software uses only the random number generation function(s) included in the payment terminal's PTS device evaluation for all cryptographic operations involving sensitive data or sensitive functions where random values are required and does not implement its own random number generation function(s).	Viking does not use any RNG (random number generator) for its encryption functions. Viking application does not generate nor use any random numbers for cryptographic functions.

B.2.9	The integrity of software prompt files is protected in accordance with Control Objective B.2.8.	All prompt displays on the Viking terminal are encoded in the application and no prompt files are present outside the application. No prompt files outside the Viking payment application exist, all necessary information is generated by the application.
B.5.1.5	Implementation guidance includes instructions for stakeholders to cryptographically sign all prompt files.	All prompts display on the Viking terminal are encoded in the application and no prompt files are present outside the application. No prompt files outside the Viking payment application exist, all necessary information is generated by the application

15. PCI Secure Software Standard Requirements Reference

Chapters in this document	PCI Secure Software Standard Requirements	PCI DSS requirements
2. Secure Payment Application	B.2.1 6.1 12.1 12.1.b	2.2.3
3. Secure Remote Software Updates	11.1 11.2 12.1	1&12.3.9 2, 8, & 10
4. Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data	3.2 3.4 3.5 A.2.1 A.2.3 B.1.2a	3.2 3.2 3.1 3.3 3.4 3.5 3.6
Authentication and Access Controls	5.1 5.2 5.3 5.4	8.1 & 8.2 8.1 & 8.2
Logging	3.6 8.1 8.3	10.1 10.5.3
Wireless Network	4.1	1.2.3 & 2.1.1 4.1.1 1.2.3, 2.1.1,4.1.1
Network Segmentation	4.1c	1.3.7
Remote Access	B.1.3	8.3
Transmission of Cardholder Data	A.2.1 A.2.3	4.1 4.2 2.3 8.3
Viking Versioning Methodology	11.2 12.1.b	
Instructions for customers about secure installation of patches and updates.	11.1 11.2 12.1	

16. 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.
3DES	In cryptography, Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.
Merchant	The end user and purchaser of the Viking product.
SSF	The PCI Software Security Framework (SSF) is a collection of standards and programs for the secure design and development of payment software. Security of payment software is a crucial part of the payment transaction flow and is essential to facilitate reliable and accurate payment transactions.
PA-QSA	Payment Application Qualified Security Assessors. QSA company that provides services to payment application vendors to validate vendors' payment applications.
SAD (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.
HSM	Hardware security module

17. Document Control

Document Author, Reviewers and Approvers

Description	Function	Name
PA-QSA	Reviewer	Claudio Adami / Flavio Bonfiglio Sorans
Development	Author	Aruna Panicker
Compliance Manager	Reviewer & Approver	Arno Ekström
System Architect	Reviewer & Approver	Shamsher Singh
QA	Reviewer & Approver	Varun Shukla
Product Owner	Reviewer & Approver	Cecilie Jenssen Tyldum / Arto Kangas
Product Manager	Reviewer & Approver	May-Britt Denstad Sandersnäs
Engineering Manager	Manager	Taneli Valtonen

Summary of Changes

Version Number	Version Date	Nature of Change	Change Author	Reviewer	Revision Tag	Date Approved
1.0	03-08-2022	First Version for PCI-Secure Software Standard	Aruna Panicker	Shamsher Singh		18-08-22
1.0	15-09-2022	Updated section 14 with the not-applicable control objectives with their justification	Aruna Panicker	Shamsher Singh		29-09-22
1.1	20-12-2022	Updated sections 2.1.2 and 2.2 with Self4000. Removed Link2500 (PTS version 4.x) from the supported terminal list	Aruna Panicker	Shamsher Singh		23-12-22
1.1	05-01-2023	Updated section 2.2 with Link2500 (pts v4) for continuing the support for this terminal type.	Aruna Panicker	Shamsher Singh		05-01-23
1.2	20-03-2023	Updated section 2.1.1 with Latvian and Lithuanian terminal profiles. And 2.1.2 with BT-iOS communication type support	Aruna Panicker	Shamsher Singh		

Distribution List

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

Document Approvals

Name	Function
Cecilie Jenssen Tyldum	Product Owner
Arto Kangas	Product Owner

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