Digital Payments
for a Trusted World

WORLDLINE

WL Samport POS software implementation guide v1.1.6

Department:	In-Person Payments
Document Date:	2025-05-14
Classification:	For public use
Version:	1.1.6
Previous version:	-

Version history

Rev.	Pages	Description	Date and sign
b4	All	New document	2023-02-15 - DS
b5	13	Information about where to find ECR REST API specification.	2023-02-17 - DS
b6	11 12	Added PTS PCI approval number and firmware number. BT not supported by the REST API.	2023-02-23 - DS
b7	24	Added key life instructions.	2023-02-24 - MJ
1.0	25 17	Added parameter integrity instructions. Added info about masked PAN during manual entry	2023-03-20 - MJ
1.1.0	8	Added section PCI SSC.	2023-02-01 - DS
1.1.1	19-25	Adjusted the security usage section.	2024-04-08 - DS
1.1.2	5	Added WL Samport POS information, 1.0.21+7133.1.0.0.	2024-05-20 - DS
1.1.3	5, 13, 14	New WL Samport POS software 1.0.22+7148.1.0.0	2024-07-03 - DS
1.1.4	5, 13, 14	New WL Samport POS software 1.0.23+7181.1.0.0	2025-04-08 - DS
1.1.5	5, 13, 14	New WL Samport POS software 1.0.24+7188.1.0.0	2025-04-15 - DS
1.1.6	5, 13, 14	New WL Samport POS software 1.0.26+7192.1.0.0	2025-05-14 - DS

Table of contents

1 Terminal software version ... 5

2 Abbreviations ... 6

3 Introduction ... 7

4 PCI SSC ... 8

5 General description of the products ... 9
5.1 MOVE/5000 ... 9
5.2 LANE/3000 ... 10
5.3 The payment flow – Move/5000, Lane/3000 (Host2T2/REST API, Stand-alone) ... 11

6 Requirements ... 13
6.1 Stand-alone ... 13
6.1.1 Hardware Requirement 13
6.1.2 Software requirement 13
6.2 Integrated ... 14
6.2.1 Hardware requirement 14
6.2.2 Software requirement 14
6.2.3 Network & services requirement 14

7 Implementation ... 15
7.1 Application versioning methodology ... 16
7.2 Secure delivery of remote payment application updates ... 17
7.3 Application updates from TMS ... 17

8 Support ... 18

9 Security usage ... 19
9.1 Account data protection ... 19
9.2 Delete any sensitive authentication data gathered as a result of troubleshooting the payment application ... 20
9.3 Delete cryptographic key material or cryptograms stored by previous payment application versions ... 20
9.4 Cardholder data protection: mask PAN ... 20
9.5 Access to critical assets is authenticated ... 20
9.6 Access to critical assets requires unique identification ... 21
9.7 By default, all access to critical assets is restricted to only those accounts and services that require such access ... 21
9.8 All activity is captured in sufficient and necessary detail to accurately describe the specific activities that were performed, who performed them, the time they were performed, and the critical assets that were affected ... 21
9.9 The software supports secure retention of detailed activity records. ... 21
9.10 Attacks are detected, and the impacts/effects of attacks are minimized. ... 21
9.11 Activity tracking settings ... 22
9.12 Securely Implement Wireless Technology ... 22
9.13 Cardholder data must never be stored on a server connected to the internet ... 23
9.14 Facilitate secure remote access to payment application ... 23
9.15 Use of multi-factor authentication ... 24
9.16 Use of Cryptography ... 24

9.17 PIN shield ... 25
9.18 Skimming prevention ... 25
9.19 Keep the device parameters up to date ... 25
9.20 Secure Defaults ... 26

1 Terminal software version

Software version	PCI Secure SW Standard impact	Description
WL Samport POS 1.0.21 Security version: 1.0.0	High	-PCI Secure Software Standard 1.1 validated. -Application name changed to WL Samport POS. -Application selection using the yellow button for both contact and contactless transactions. -Multi-user support for the ECR REST API.
WL Samport POS 1.0.22 Security version: 1.0.0	No-Impact	-Application selection using the yellow button for both contact and contactless transactions. -Multi-user support for the ECR REST API. -Fixed an issue in version 1.0.21, using automatic application selection with a co-badged Dankort/Visa card. -Ignoring the choice of bypass PIN instead of declining transactions. -Replaces 1.0.21.
WL Samport POS 1.0.23 Security version: 1.0.0	No-Impact	-Only released to pilots. Replaced by 1.0.24.
WL Samport POS 1.0.24 Security version: 1.0.0	No-Impact	-Replaced by 1.0.26.
WL Samport POS 1.0.26 Security version: 1.0.0	No-Impact	-Resolved an issue where a transaction was not cancelled if a cancel request was submitted within 300 ms. -An descriptive text is added on the screen indicating that the yellow button should be used to activate application selection.

2 Abbreviations

3DES	= Triple Data Encryption Standard. Aka TDES
BT	= Bluetooth
CHD	= Card Holder Data
CDE	= Cardholder Data Environment
DUKPT	= Derived Unique Key Per Transaction
E2EE	= End To End Encryption
ECR	= Electronic Cash Register
IPSEC	= Internet Protocol Security
MAC	= Message Authentication Code
NAT	= Network Address Translation
PA-DSS	= Payment Application Data Security Standard
PAN	= Primary Account Number
PAT	= Port Address Translation
PCI	= Payment Card Industry
PCI DSS	= PCI Data Security Standard
PCI PTS	= PCI PIN Transaction Security
PCI SSC	= Payment Card Industry Security Standards Council
PDA	= Personal Digital Assistant (e.g. smartphone)
PIN	= Personal Identification number
PTS	= PIN Transaction Security
RADIUS	= Remote Authentication and Dial-In User Service
SAD	= Sensitive Authentication Data
SPS	= Secure Payment Service
SRED	= Secure Reading and Exchange of Data
SSH	= Secure Shell
SSL	= Secure Sockets Layer
TACACS	= Terminal Access Controller Access Control System
TCP/IP	= Transmission Control Protocol / Internet Protocol
TLS	= Transport Layer Security
TMS	= Terminal Management System
VPN	= Virtual Private Network
WEP	= Wired Equivalent Privacy
WPA	= Wi-Fi Protected Access

Cardholder Data (CHD)	Sensitive Authentication Data (SAD)
Primary Account Number	Full Track Data
Cardholder Name	CAV2/CID/CVC2/CVV2
Service Code	PIN/PIN Block
Expiration Date	

3 Introduction

Bambora Device has developed a payment application called WL Samport POS that resides within the terminals from the manufacturer Ingenico. This is an implementation guide for the Bambora Device Ingenico terminals.

It is a complementary document to any additional protocol documents that are used for integrating an external ECR application connected to the terminal. This document must be read before the integration is started.

This Implementation Guide should be disseminated to all relevant application users including merchants and resellers/integrators. The guide should instruct merchants, resellers and integrators how to install the Bambora Device products in a PCI Secure Software Standard 1.1 compliant manner. It is not intended to be a complete installation guide. 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 PCI Secure Software Standard.

Updates to the Implementation Guide can be obtained by contacting the technical support. (See chapter Support for contact information) or by downloading from the Partner community.

Note! If you do not follow the steps outlined in this Implementation Guide, your installation will not be PCI Secure Software Standard compliant.

4 PCI SSC

The PCI SSC stands for Payment Card Industry Security Standards Council. It’s a global organization created to develop, enhance, promote and assist with the understanding of security standards for payment security. The council was founded by major credit card companies such as Visa, MasterCard, American Express, Discover and JCB International to improve payment security throughout the transaction process.

The primary purpose of the PCI SSC is to oversee the ongoing development and management of the PCI Security Standards, which includes the PCI Secure Software Standard. PCI Secure Software Standard is a part of the PCI Software Security Framework (SSF). The security requirements defined within the PCI Secure Software Standard ensure that payment software is designed, engineered, developed and maintained in a manner that protects payment transaction data, minimizes vulnerabilities and defends against attacks. The WL Samport POS is listed on the PCI SSC’s list of validated payment software:
https://listings.pcisecuritystandards.org/assessors_and_solutions/payment_software

Another important PCI standard is the PCI DSS (PCI Data Security Standard). This standard applies to all entities that store, process or transmit cardholder data and/or sensitive authentication data. It's designed to protect cardholder data by ensuring service providers maintain a secure transaction environment. Bambora Device AB is annually being validated by a QSA to comply with the PCI DSS requirements.

The PCI SSC's standards will help maintain the security of the payment card ecosystem and contribute to the trust and confidence of consumers worldwide.

5 General description of the products

The payment application will run on terminal hardware from the manufacturer Ingenico based on the Telium Tetra OS. The same application runs on 2 different terminal models: the Move/5000 and Lane/3000, which this guide will cover.

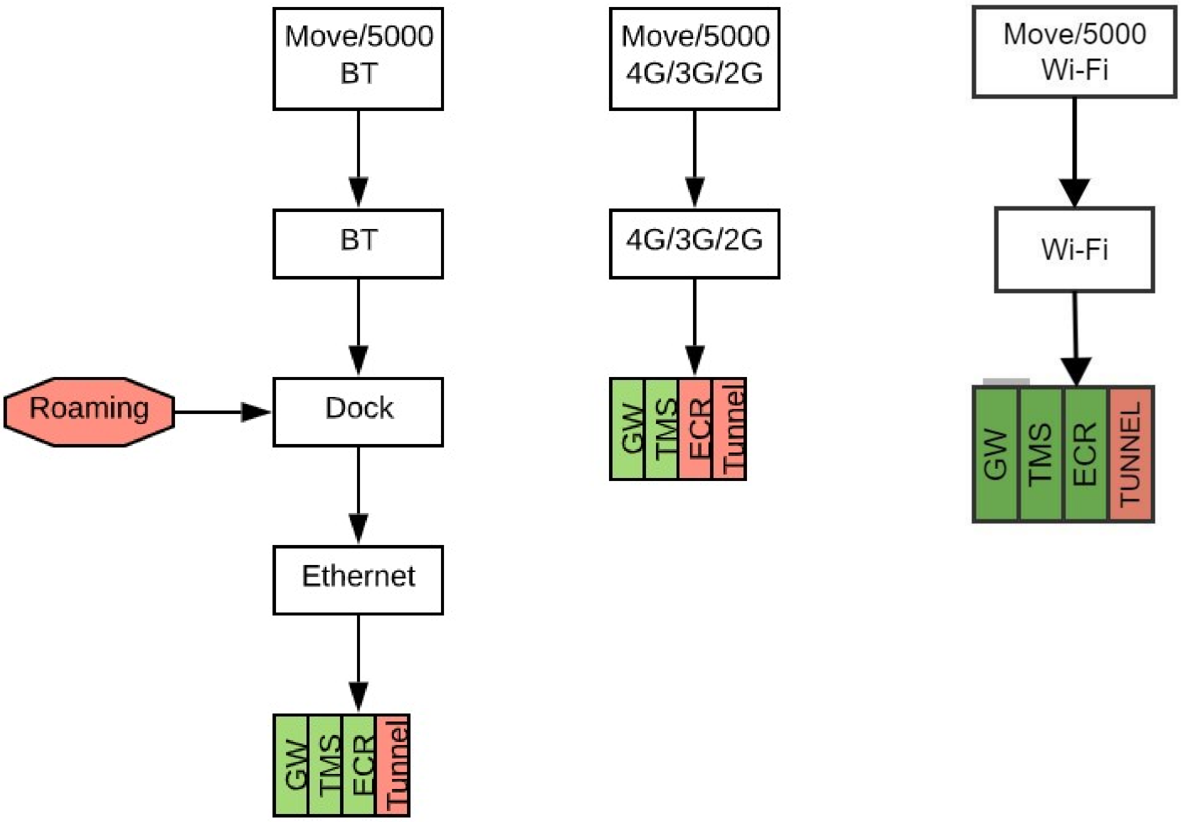
The Move/5000 can be used as a standalone terminal and has also the functionality to be connected to an ECR through Worldline Samport's own REST API protocol or Host2T version 2.x protocol, hereafter called Host2T2. Lane/3000 on the other hand is an "integrated terminal" only and must be connected to an ECR through either the ECR REST API or Host2T2. The communication between terminal and cash register is Ethernet.

The terminals communicate with Samport Payment Gateway, which is located in the PCI DSS approved card environment. The PCI PTS approved terminal hardware communicates through Ethernet, Wi-Fi or 2G/3G/4G.

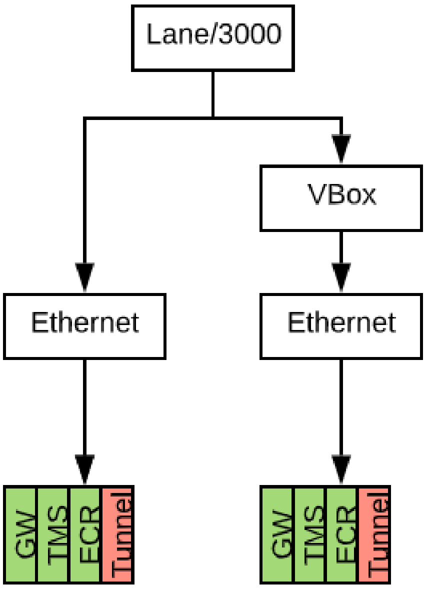
If merchants are using Wi-Fi connections in the same environment as the terminal, it's important that WPA2 (TKIP or AES) encryption is used to sustain a PCI Secure Software Standard compliant merchant environment.

The terminals have a magnetic stripe reader and a smart card reader. All models are equipped with a contactless reader, which is always enabled.

5.1 MOVE/5000



5.2 LANE/3000


Lane/3000
VBox
Ethernet
Ethernet
GW
TMS
ECR
Tunnel
GW
TMS
ECR
Tunnel

5.3 The payment flow – Move/5000, Lane/3000 (Host2T2/REST API, Stand-alone)

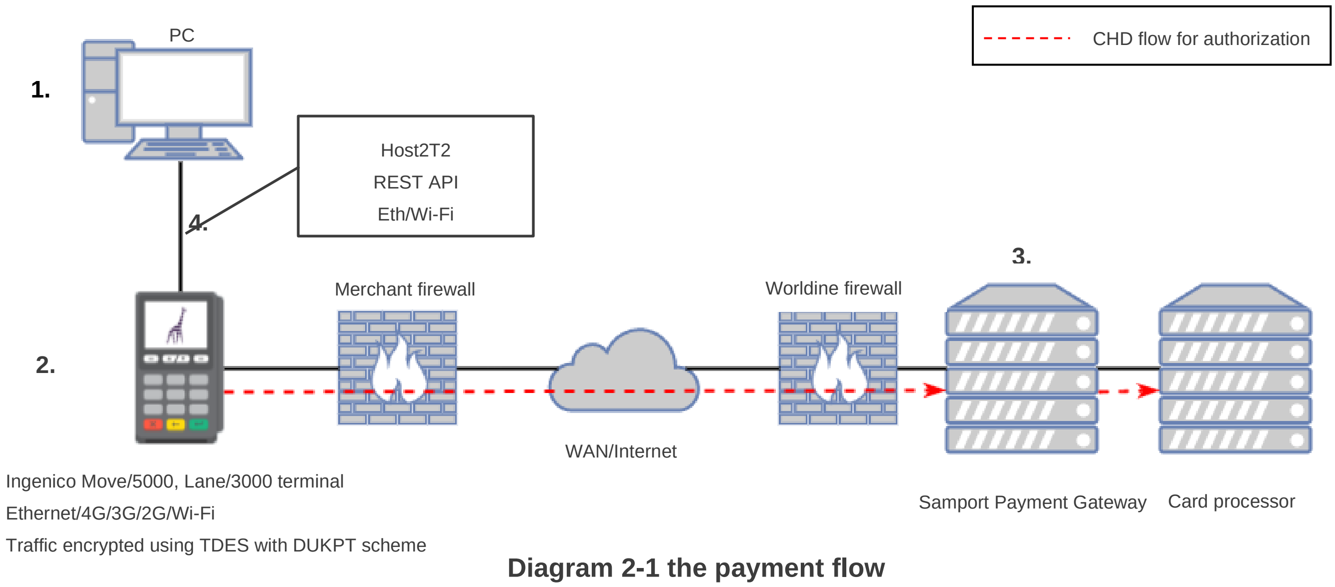


Diagram 2-1 the payment flow

1. The cashier chooses card payment in the terminal menu or by an ECR connected cash register. The cash register application contacts the terminal through selected protocol, for the type of cash register installed. It is also possible to insert the card into the card reader to initiate a transaction, when used as a stand-alone terminal.

2. The terminal will start up the card information gathering process. The terminal will display directives for the card holder what to do.
   - The cardholder will either swipe, insert or tap the card in/on the terminals integrated reader to collect the card information. Alternative the card holder will enter the PAN, expire date and CVV2 (if required by the issuer) in the terminal PED.

   - The WL Samport POS payment application in the terminal, will TDES encrypt (with DUKPT scheme) the cardholder data (CHD) and sensitive authentication data (SAD) that is gathered in the previous step. When the terminal has all the information it needs for authorization, it will contact Samport payment gateway.

3. The Samport payment gateway authorizes the payment request from the terminal against a card processor. The result from the authorization will be processed and returned to the terminal. The result sent from the processor to the terminal, contains no CHD or SAD.

   The payment application in the terminal hold the CHD and SAD in VRAM until a result is received from the processor or until the terminal times out, thereafter the CHD and SAD is purged. Before the CHD is purged, the PAN is saved truncated for receipt information, see below.

4. The terminal will show the Result on the display or if a cash register is connected the terminal will return the following information back to the cash register:

   - Response code from the bank.
   - Worldline Samport unique authorization number.
   - Bank unique authorization number.
   - Truncated PAN, only the last 4 digits. (e.g. **** **** **** 1234)
   - EMV application information.
   - Loyalty card number, bonus card number (Never Visa, Visa Electron, MasterCard, Maestro, American Express, Diners, UPI or JCB)

5. The terminal will print a receipt with truncated PAN together with other insensitive data. Alternatively, if a cash register is used, it could print a receipt instead of the terminal.

6 Requirements

The payment application is intended to be installed and used on Bambora Device POI models:
Move/5000 hardware number: MOV50BC or MOV50BQ, PCI PTS approval number: 4-20316.
Lane/3000 hardware number: LAN30EA, PCI PTS approval number: 4-30310. Security firmware version for all models: 820376v01.xx.

6.1 Stand-alone

6.1.1 Hardware Requirement

- Ingenico Move/5000. The Move/5000 is delivered with mobile network connection. To use Bluetooth or Wi-Fi, please change interface in the terminal menu. Settings > Communication > Select interface.

Configurations:	Products:	Details:
Standalone Wireless Mobile Network	Terminal: Move/5000 Config: Mobile connection 4G/3G/2G Charger base Power supply	HVN: MOV50BC or MOV50BQ Sierra sim card
Standalone Wireless BT	Terminal: Move/5000 Config: Bluetooth Bluetooth-Ethernet base Power supply Ethernet cable 3m RJ45 – RJ45	HVN: MOV50BC or MOV50BQ
Standalone Wireless Wi-Fi	Terminal: Move/5000 Config: Wi-Fi Base for charging Power supply	HVN: MOV50BC or MOV50BQ

6.1.2 Software requirement

- Bambora Device AB application WL Samport POS 1.0.26+7192.1.0.0

6.2 Integrated

6.2.1 Hardware requirement

- Move/5000, Lane/3000. The Move/5000 is delivered with mobile network connection. To be able to connect the terminal to a cash register application please change interface to Bluetooth or Wi-Fi in the terminal menu. Settings > Communication > Select interface.

Configurations:	Products:	Details:
Integrated Wireless BT	Terminal: Move/5000 Config: Bluetooth Bluetooth-Ethernet base Power supply Ethernet cable 3m RJ45 – RJ45	HVN: MOV50BC or MOV50BQ
Integrated Wireless Wi-Fi	Terminal: Move/5000 Config: Wi-Fi Base for charging Power supply	HVN: MOV50BC or MOV50BQ
Integrated Wired	Terminal: Lane/3000 Direct HDMI to Ethernet 4m Power supply	HVN: LAN30EA

6.2.2 Software requirement

- Bambora Device AB application WL Samport POS 1.0.26+7192.1.0.0
- Recommended TCP/IP port number Host2T2: 1337
- Port number for ECR REST API: 443

- Cash register with the following option (Move/5000 or Lane/3000)
    - PC Cash register application with Host2T2 support
    - PC Cash register application with Connect2T support
    - PC Cash register application with ECR REST API support (Move/5000 BT not supported.)

6.2.3 Network & services requirement

The terminals rely on having an internet connection. However, terminal connected to ethernet should not be connected directly to the Internet – it must be placed behind a firewall to prevent inbound connections from the Internet to the device. The terminals do not rely on any other services. Specify mac addresses for firewall rules.

The payment terminal requires access to Worldline's payment services in order to operate properly. It’s the merchant's responsibility to ensure that the payment terminal is allowed access to these services from the merchant’s local network. Configure your firewall to allow outgoing traffic to the following services:

- 213.232.97.35 TCP / 975-979
- 91.224.37.30 TCP / 975-979
- *.samport.com TCP / 443 (https)

Do **not** hardcode IPs for these services as they can change over time.

7 Implementation

The cash register vendor needs to implement a client application in order to establish the connection. There are two ways to integrate a Tetra terminal: the ECR REST API or via the Host2T2 protocol.

REST API: This allows for communication via web-based API calls, providing a flexible and modern approach to integration. The ECR REST API is designed to be easy to use and integrate and provides a standardized way for applications to communicate with the Tetra terminals. The REST API allows for great flexibility in terms of development and maintenance. It enables cash register applications built on different platforms and programming languages to interact with terminals without compatibility issues. It can facilitate real-time exchange of information between the cash register and terminal, ensuring that transaction data is processed and reflected instantly, which is critical in a retail environment. It’s particularly useful for scenarios where the cash register and terminal are not in the same physical location. The Swagger specification describes implementation of the ECR REST API.

Host2T2: The document “HOST2T 2.X.X Protocol Specification.pdf” is the technical specification for Host2T2 describing how to use and implement the Host2T2 protocol. Please contact the Integration Specialists to receive the latest Host2T2 documentation, the Swagger and related integration questions such as certificate, and integration key. See section Support for contact details.

7.1 Application versioning methodology

WL Samport POS is using Semantic Versioning system. https://semver.org/ Semantic Versioning communicates information regarding changes through the version number.

Exposed to customers						
Compatibility				Secure Software Standard		
Major	Minor	Patch	Build number	High	Low	Administration
X	Y	Z	b	H	L	A
Incompatible changes.	Backward compatible additions/changes.	Backward compatible bug fixes, maintenance.	Internal build number	Security impact and/or any Secure Software Requirement	No impact on security but affects Secure Software Standard requirements.	Administrative changes to the Payment Software listing.

Format: X.Y.Z+b.H.L.A

Major (X) = Incompatible changes that affects implementation of cash register integration.
Minor (Y) = Backwards compatible functionality towards cash register integration.
Patch (Z) = Maintenance release with backwards compatible bug fixes.
Build number (b) - Internal build number. All releases regardless of X, Y, Z have a unique value of b.
A change of the number X, Y, Z, b may not lead to an increase of the H, L or A.

Security:
High (H) = Changes when full Secure Software Assessment was required prior to release. An increase of the number (H) have an impact on security of the application and/or any Secure Software Requirement.
Low (L) = A delta Secure Software Standard assessment was required prior to release. No impact on security but affects Secure Software Standard requirements or it's dependencies.
Administration (A) = No software changes, but any changes to how the Payment Software is described in the List of Validated Payment Software, for example, corporate identity or software name changes. Submitted to PCI SSC via the Secure Software Assessor Company for review.
A change of the number H, L and A will always impact the Payment Software listing.

Seven numeric elements, X, Y, Z, b, H, L and A where X, Y, Z and b, H, L, A are dot separated. The format separator between Z and b is +. Each element can consist of up to 6 digits.

Examples:

1.0.22+2312.1.0.0 -Payment Software listing: 1.0.0
1.1.0+8956.1.1.0 -Minor changes with Low impact changes. Payment Software listing: 1.1.0

Major (X)	Minor (Y)	Patch (Z)	Build number (b)	High (H)	Low (L)	Administration (A)
	X		X		X	

1.0.25+8372.1.0.0 -Payment Software listing: 1.0.0
2.0.0+3748.1.0.0 -Incompatible change (Major) with increase of the number X, but no impact on the security or/and Secure Software Requirement, which does not affect the Payment Software listing. Payment Software listing: 1.0.0

Major (X)	Minor (Y)	Patch (Z)	Build number (b)	High (H)	Low (L)	Administration (A)
X			X			

7.2 Secure delivery of remote payment application updates

The WL Samport POS application does not support remote payment application updates. All updates are downloaded by the application itself from a TMS.

7.3 Application updates from TMS

The WL Samport payment application is distributed to the terminal in a secure manner. The terminal retrieves the software from Samport TMS using either a proprietary protocol called Datax 2 or using HTTPS and the connection is secured using TLS 1.2 encryption.

Before the new application is upgraded in the terminal, the application signature is verified by the PCI PTS approved terminal hardware to make sure it's a software allowed to run on the terminal. Only software that has been signed with the proper Bambora Device key is allowed to exist and run in the terminal.

Information of a new update is sent out prior to the release to relevant parties so that testing of ECR connections can be performed.

Automatic software updates are usually delivered to the terminal after a settlement has been done. The automatic update is handled by Bambora Device centrally and the merchant does not need to do anything to get new updates.

If you want to update the terminal manually, please follow these steps on the terminal:

1. Press menu button
2. Press Support…
3. Press Terminal mgnt…
4. Press Software update
5. Please allow time for the terminal to download the software
6. The new software has been downloaded and the terminal is ready for use again

If there are any questions please contact our support, the contact details can be found in chapter Support.

8 Support

Questions regarding the implementation of the Ingenico models, please contact Integration Specialists at integration.support@worldline.com. The Worldline Samport Partners can find the latest implementation guide on the Partner Community. Contact for replacement or destruction of terminals: Worldline Customer Service at support.nordics@worldline.com or +46(0)10-10 66 000, between 9.00-20:00 (GMT+1) on non-holiday weekdays and 10:00-14:00 on Saturdays.

9 Security usage

The Move/5000 and Lane/3000 terminal models from Ingenico must be used according to the Payment Card Industry (PCI) Secure Software Standard. By using these products means that you have accepted and follow the PCI DSS and PCI Secure Software Standard. Please visit https://www.pcisecuritystandards.org/ for the standards.

The following chapters describe how the terminals must be used in order to comply with Secure Software Standard and PCI DSS version 3.2.

9.1 Account data protection

Resellers and merchants applicability:
SAD has never been stored by any version of the WL Samport POS application. The application does not store any card validation codes, magnetic stripe data, PIN's or PIN blocks neither before, nor after authorization, it is only held in the RAM, and the PA does not send this data to the ECR cash register.

The terminal will remove the SAD after the transaction has been acknowledged by the gateway. SAD is never stored, it is only held in the RAM. For offline transactions PAN and expiry date is stored encrypted with 128-bit DUKPT TDES cipher in the terminal database, SAD is excluded. Once the authorization procedure is successfully completed, the encrypted PAN and expiry date is purged from the terminal database. Encrypted PAN and encrypted expire date may be printed for offline transactions on the merchant receipt for the purpose of manual transaction recovery in case of a terminal failure before settlement.

For online transactions only the 4 last digits of the PAN is stored (masked PAN) in the terminal database. Once the settlement is completed, the transaction data is purged from the database.

The terminals clear all transaction data from the memory when a register closing is done. Before installing a new version to the Ingenico terminal, make a register closing to remove transaction data from the terminal. The terminal will not update before this has been performed. The TMS does not collect any account data, logs contain only errors and systems messages.

The software does not disclose sensitive data through any unintended channels.

If cardholder data is obtained it shall be deleted in a secure manner when the data is no longer required for legal, regulatory, or business purposes.

For terminals connected to windows PC cash registers, it is recommended that the system restore is disabled for security purposes. The cash register shall never store encrypted cardholder data (received from the terminal) and it shall not accept input or store cardholder data.
Follow the instruction below:

Steps to turn off System Restore (Windows 11)

1) Right-click the My Computer icon on the desktop and click Properties.
2) Go to the System Protection tab and click Configure.
3) Select Disable system protection and click OK.
4) Click Yes.
5) In the System Properties window, click OK.
6) Restart your PC.

9.2 Delete any sensitive authentication data gathered as a result of troubleshooting the payment application

Resellers and merchants applicability:
Sensitive authentication data is not stored by the terminal during transactions or when used for trouble shooting. Worldline does not need SAD for trouble shooting. As a merchant, partner or support person you shall never try to log or collect SAD.

User interaction is not required for any cardholder data protection, sensitive data is not retained as part of transaction or collected as part of troubleshooting logs or traces. (A.2.3.b)

9.3 Delete cryptographic key material or cryptograms stored by previous payment application versions

Resellers and merchants applicability:
PAN and expiry date for offline transactions are stored encrypted with 128-bit DUKPT TDES cipher in the terminal database. Historic data should be removed according to 2.4.d requirement of Secure Software Standard; therefore, no historic data will need to be re-encrypted. Cryptographic material is removed when any online transaction is performed and as soon as the terminal has connection.

9.4 Cardholder data protection: mask PAN

Resellers and merchants applicability:
The terminals always truncate the PAN when it comes to the card brands Visa, Visa Electron, MasterCard, Maestro, American Express, Diners, China Union Pay and JCB. The PAN is truncated on all digits except the four last e.g. **** **** **** 1234 and displayed masked on the receipt, on the screen and sent in the communication between the terminal and the ECR cash register.

The masked PAN can be found on receipts and transaction reports of the terminal.

Unmasked PAN are never shown, communicated or printed and it is not possible to configure the terminal to show full PAN.

9.5 Access to critical assets is authenticated

Resellers and merchants applicability:
There are no user accounts on the Ingenico terminals. Therefore, there is no access to any cardholder data. This requirement is not applicable to any merchant or reseller using the terminal.

9.6 Access to critical assets requires unique identification

Resellers and merchants applicability:
The WL Samport POS and the terminal database don't have any user IDs at all. The user has not the possibility to logon on to any cardholder data environment using Bambora Device Ingenico terminals.

9.7 By default, all access to critical assets is restricted to only those accounts and services that require such access

Resellers and merchants applicability:
This requirement is not applicable to any merchant or reseller using the terminal.
User accounts or authentication credentials is not supported by the application. Access to critical assets is not provided in the terminal nor stopping or pausing of sensitive functions. Usage of or changes to sensitive functions is only allowed by the software itself. PCI Secure Software Standard, Control objectives 5.3, 5.4 and 8.1.

9.8 All activity is captured in sufficient and necessary detail to accurately describe the specific activities that were performed, who performed them, the time they were performed, and the critical assets that were affected

Resellers and merchants applicability:
This requirement is not applicable to any merchant or reseller using the terminal.
No accounts or authentication credentials are supported by the software and the application does not offer any access to critical assets to the customer. PCI Secure Software Standard 1.2, Control objective 8.2.

9.9 The software supports secure retention of detailed activity records.

Resellers and merchants applicability:
This requirement is not applicable to any merchant or reseller using the terminal.

User interaction is not possible to enable or change application's security controls, including logging functionality. No third-party systems are used when handling log files. PCI Secure Software Standard, Control objective 8.3.

9.10 Attacks are detected, and the impacts/effects of attacks are minimized.

Resellers and merchants applicability:
This requirement is not applicable to any merchant or reseller using the terminal.
The software does not rely on third-party tools or services to provide attack detection capabilities.

Only signed payment application software packages can be installed into the POI. PCI Secure Software Standard, Control objective 9.

Activity tracking and software files integrity is supported by the terminal itself and does not require any user interaction for enabling or configuration.

9.11 Activity tracking settings

Resellers and merchants applicability:
PCI Secure Software Standard requirement 8. The payment application for the Ingenico terminals has logging activated by default. There is no available setting to turn the logging off. If logging is somehow prevented or disabled, the merchant will be non-compliant with PCI DSS.

The payment application utilizes centralized logging and sends the log files to a central server at Bambora Device. The merchant may collect the logs from the centralized storage and processing according to Secure Software Standard and PCI DSS requirements, contact Worldline to receive instructions on how to collect the log files, see section Support for contact details.

There are no user accounts in the payment application, hence no user interaction is required to configure, initiate or restart logging. PCI Secure Software Standard, control objective 8.3. b.

Logging mechanisms and the ability to track activities are critical in determining the cause of an error. The presence of logs in all environments allows thorough tracking and analysis when something does go wrong. Logging must therefore also be implemented in the cash register application to track activities from and to the cash register application which can be used as assistance if problems are experienced.

9.12 Securely Implement Wireless Technology

Resellers and merchants applicability:
A typical installation of a Bambora Device terminal is that the PTS approved terminal handles all the communication with the Samport Payment Gateway through following methods:

- 4G/3G/2G: The terminal communicates with payment gateway via the 4G/3G/2G network.
- Bluetooth: The terminal communicates with payment gateway via a BT access point and merchant network connection.
- Ethernet: The terminal communicates with payment gateway via merchant’s LAN/Ethernet.
- Wi-Fi: The terminal communicates with payment gateway via merchant’s Wi-Fi network.

The WL Samport POS application does not send any clear text cardholder data or have any remote access to cardholder data over any media and the application does not handle the communication, this is done by the PCI PTS approved terminal hardware.

If the merchant uses a wireless network, make sure the wireless connections are securely implemented. Minimum wireless settings and configurations that must be in place:

- All wireless networks must use a firewall and logging must be switched on.
- Change encryption keys (WPA2/WPA3) from default at installation
- Change the default SSID
- Disable SSID broadcast

- Ensure strong password by using a combination of capital and lowercase letters, numbers, symbols and at least 8 characters long.
- Default passwords/phrases on access points and wireless connections are required to be changed upon installation.
- Default SNMP community strings are also required to be changed upon installation.
- Change other security-related wireless vendor defaults
- Change encryption keys (WPA2/WPA3) anytime anyone with knowledge of the keys leaves the company or changes positions.
- Make sure wireless access points are updated to the latest firmware
- Use at least WPA2 with strong key only.
- WEP is prohibited to use.

According to the PCI DSS 4.0 Requirement:
2.3 Wireless environments are configured and managed securely.

If the merchant does not follow these requirements, the terminal is not PCI DSS compliant.

9.13 Cardholder data must never be stored on a server connected to the internet

Resellers and merchants applicability:
The WL Samport POS application does not store any cardholder data after an authorization. All authorizations are encrypted with 3DES DUKPT. Only encrypted PAN and expire date is stored (encrypted with 3DES DUKPT), on the terminals secure flash memory, for offline transactions until they are sent to the Samport payment gateway. Once the terminal has gotten an acknowledgement from the gateway on the sent authorization message, it will erase the data.

The terminal must not be connected directly to the Internet – it must be placed behind a firewall which prevents inbound connections from the Internet to the device. Accessing the cardholder data in the terminal from the internet is not possible. If the terminal is opened by external physical attack then the self-destruction mechanism will be activated and the terminal will erase all keys. The terminal will not be able to operate without any keys, the terminal must be sent to Worldline, and Ingenico to be repaired and to be formatted so new keys could be injected.

If the message “Irruption” is shown on the terminal screen the terminals has been compromised and must not be used, please contact Worldline support immediately and report this, the contact details can be found in section Support.

9.14 Facilitate secure remote access to payment application

Resellers and merchants applicability:
The Ingenico terminal does not support remote access to the payment application. This requirement is not applicable to integrators using the terminals.

9.15 Use of multi-factor authentication

Resellers and merchants applicability:
The WL Samport POS application cannot be accessed remotely. If remote access to any cardholder data environment outside of the application is configured, secure use of multi-factor authentication for all individual non-console administrative access and all remote access to the CDE.

Extracts from PCI DSS 4.0 requirements:
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.

9.16 Use of Cryptography

Resellers and merchants applicability:
PCI Secure Software Standard requirement 6 and 7. The WL Samport POS application with Ingenico firmware and Bambora Device handles all the key management on behalf of the merchant. Therefore, no user instructions were given throughout this document as the entire key management process is fully supported by Worldline.

Bambora Device AB does all the handling and generation of the keys in a secure manner and follows the standards set by the industry by implementing these rules and processes:

- Document every key and custodian.
- Restrict access to keys to the fewest number of custodians necessary.
- Generation of strong cryptographic keys.
- Store keys securely in the fewest possible locations and forms.
- Secure cryptographic key distribution.
- Secure cryptographic key storage.
- Cryptographic key changes for keys that have reached the end of their crypto period.
- Prevention of unauthorized substitution of cryptographic keys.
- Destroy old/unused keys in a safe manner.

The cryptographic keys are stored on the secure memory of the PTS approved terminal and are not accessible.

The terminals are to be considered valuables and should be in a locked location when not used. When the terminals have reached sun set date and shall not be used any more the terminal shall be destroyed in a secure manner. If the merchant or reseller cannot provide this, the terminal can be sent to Worldline for destruction. Please contact our support (contact details can be found in section Support).

VISA, Mastercard and other brands distribute their Certification Authority Public Keys to acquirers for use in terminals. These are used for generating cryptograms during EMV transactions. Should a private key at a brand be exposed, that brand will issue a replacement public key, which will be installed on the next parameter update (the CAPUB parameter).

The terminal uses Derived Unique Key Per Transaction (DUPKT) technology to encrypt sensitive and other data. This technology depends on root key. Should all root key be exposed, or a derived key, the terminal must be replaced. The root key can be installed only from within a secure Worldline facility.

If the DUKPT runs out of unique keys, the terminal must be replaced. The symptom is that all transactions are declined. The DUKPT-generated key consists of a prefix and a 20-bit transaction counter, which yields 1 048 576 unique keys. Depending on features, the terminal may use more than one key per transaction, let us say

1.2, so the estimated lifespan is around 874 000 transactions. If a terminal makes 10 transactions per day, its estimated lifespan is therefore 87 400 days = 240 years. If a terminal makes 100 transactions per day, its estimated lifespan is 24 years.

9.17 PIN shield

Resellers and merchants applicability:
Move/5000 is a handheld device without privacy shield. The Lane/3000 terminals are equipped with factory mounted pin shields. The privacy shield of the PIN pad has been approved in accordance with requirements in PCI PTS POI. In accordance to BankAxept – POS Security Requirements v2p2 (SEC-HW-03), Merchants shall instruct customers to use Move/5000 terminal in intended manner, handheld by the cardholder when entering PIN.

9.18 Skimming prevention

Resellers and merchants applicability:
To protect devices form tampering and substitution:

- Maintain a list of devices
- Regularly inspect devices to look for tampering or substitution
- Regularly inspect areas to discover cameras directed at the PIN entry on the payment terminal
- Train personnel to be aware of suspicious behavior and to report tampering or substitution of devices

Extracts from PCI DSS 4.0 requirements:
9.5.1.1 An up-to-date list of POI devices is maintained, including:
• Make and model of the device.
• Location of device.
• Device serial number or other methods of unique identification.

9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.

Best practices on skimming prevention are available on the PCI SSC website.

9.19 Keep the device parameters up to date

Resellers and merchants applicability:
The device maintains its integrity by checking parameters' content and origin before install, so that parameters from outside Worldline cannot be installed, and by periodically checking for updated parameters, for example after end-of-day settlements. To ensure the device remains up to date, avoid shutting down the device or Internet access too soon after the settlement, at least a few seconds.

Extracts from PCI SSF 1.1 requirements:
9.1.a … the software validates the integrity of its own executable and configuration, files, and datasets that it relies upon for operation (such that unauthorized, post-deployment changes can be detected).

9.20 Secure Defaults

Resellers and merchants applicability:
The WL Samport POS payment application is tested before every custom or entire base code release, if released with known vulnerabilities related to the software, programming language, third-party APIs, protocols or interfaces, users are updated with the mitigation plan. However, the application packages and files are handled only by Worldline and there is no required user interaction or action to enable those security controls or maintain them.

The WL Samport POS application does not provide users with accounts or access. Vulnerabilities related to authentication and access are not relevant to the application.