Payments to grow your world

WORLDLINE

Samport AX software implementation guidance v1.1.7

Status	Complete
Document date:	11 July 2025
Classification:	Public
Version:	1.1.7

Version history

Version no.	Version date	Status	Edited by	Most important edit(s)
1.0	22 March 2024	Complete	DS	New document.
1.1	10 April 2024	Complete	DS	SSF requirements. Changes together with QSA.
1.1.1	27 August 2024	Complete	DS	New terminal pictures.
1.1.2	23 September 2024	Complete	DS	Page 17, email address to Integration. Specialists. Page 9: Added information about differences between DX8000-5 and DX8000-2.
1.1.3	25 September 2024	Complete	DS	Page 5, 11, 12. Added Samport AX 1.0.1+3382.1.0.0. Corrected port number to 8080.
1.1.4	30 September 2024	Complete	DS	Page 5. Added listing reference number.
1.1.5	12 December 2024	Complete	DS	Page 5, 11, 12. Added Samport AX 1.3.0+3898.1.0.0.
1.1.6	25 March 2025	Complete	DS	Page 5, 11, 12. Added Samport AX 1.4.0+4582.1.0.0.
1.1.7	11 July 2025	Complete	DS	Page 5, 11, 12. Domain and IP address added to the Network & Services requirement section at page 13. Changed DX8000-5 to DX8000 where applicable. Added Samport AX 1.5.0

Table of contents

Terminal software version

Software version	PCI Secure SW Standard impact	Description
Samport AX 1.0.0 Security version: 1.0.0	High	PCI Secure Software Standard 1.2 validated. Reference number: 24-47.00794.002.
Samport AX 1.0.1 Security version: 1.0.0	No-Impact	First public release of the smart POS Axium terminals DX8000 and RX5000!
Samport AX 1.3.0 Security version: 1.0.0	No-Impact	Tip summary is added to the End of day and Totals report. Ability to view and print latest 10 end of day reports, New terminal menu layout. Tip settings can be adjusted directly from the terminal menu. A troubleshooting guide is implemented. The password requirement has been removed, with the addition that password protection can be enabled if needed. New options to cancel transactions. A start-up process implemented.
Samport AX 1.4.0 Security version: 1.0.0	No-Impact	-ReadCard support for the ECR REST API. -The operation ID is no longer needed for mirroring the terminal display. -A new endpoint has been added to the ECR REST API that allows retrieval of the dialog without requiring an operation ID. -A new switch is added to the terminal display for application selection activation.
Samport AX 1.5.0 Security version: 1.0.0	No-Impact	-Support for Smart POS app store. -The DX8000 terminal now features an alternative operating mode with clear graphics, adjustable volume and headphone connectivity to support the European Accessibility Act's goal of creating a more inclusive society. -A new endpoint has been added to the ECR REST API for modeless abort requests without the need for an operation ID. -A new receipt type has been introduced, and it's easy to use because it is divided into separate sections and formatted to a specified receipt width. -The manual application selection switch, added in version 1.4.0, has been replaced with a checkbox on the left side of the header area.

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	

Introduction

We are thrilled to introduce *Samport AX*, a payment application engineered exclusively for the Android based Ingenico Axium platform. The payment application is developed in collaboration with industry professionals, ensuring the needs of both merchants and customers are met with elegance and expertise. A payment software delivering a superior payment experience with every transaction. Empower your clients with the next generation of payment technology that's secure, simple, and user-oriented.

This is an implementation guidance for the Bambora Device Ingenico Axium terminals DX8000-5 and RX5000. The DX8000-5 will hereafter be referred to as DX8000. It's 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 guidance should be disseminated to all relevant application users including merchants, resellers and integrators. The guide instructs merchants, resellers and integrators how to install the Bambora Device products in a PCI Secure Software Standard 1.2 compliant manner and should thereby facilitate and support PCI compliance. It's not intended to be a complete installation guide. It's updated at least annually and after software changes. The annual review and updates will include new software changes (if any) as well as changes in the PCI Secure Software Standard.

Updates to the Implementation Guidance can be obtained by contacting the Integration Specialists. (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 Guidance, your installation will not be PCI Secure Software Standard compliant.

3.1 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 Samport AX 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.

General description of the products

The payment application Samport AX run on terminal hardware from the manufacturer Ingenico. The smart POS terminals are using the Axium OS based on Android. The same application runs on two different terminal models: the DX8000 and RX5000, which this guide will cover.

The DX8000 can be used as a standalone terminal or connected to an ECR through Worldline Samport's REST API protocol. RX5000 need to be connected to an ECR through REST API. The supported connectivity between the terminal and cash register is either ethernet or Wi-Fi.

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

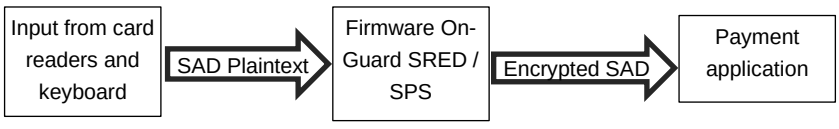
If merchants are using Wi-Fi connections in the same environment as the terminal, it's important that at least WPA2 is used to sustain a PCI Secure Software Standard compliant merchant environment.

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

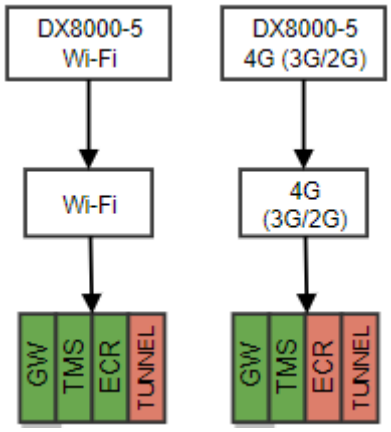
4.1 The SRED OnGuard and Ingenico Secure Payment Service module (SPS)

The payment application resides on a PTS POI terminal. The Ingenico OnGuard supported in SRED encrypts all sensitive cardholder data at the point of swipe, insertion, or tap. All the encryption occurs in the terminal's Secure Reading and Exchange of Data (SRED) module and decrease vulnerability to cybercriminal attacks. It helps reduce risk and certification scope by not letting the payment application handling sensitive data.

The Ingenico Secure Payment Service (SPS P2PE Domain 2 Certified Module) provides a gateway to the secure payment functionality of the terminal, including key management, manual entry, magstripe entry, EMV processing, PIN entry and OnGuard encryption.

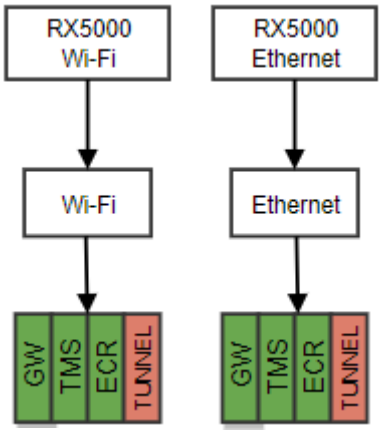


4.2 DX8000



The DX8000-5, called DX8000 in this document. Ingenico also has another DX8000, called DX8000-2 that we don't use. The DX8000-2 screen size is 5.5" instead of 6", has smaller battery, less memory, and only 2.4 GHz Wi-Fi.

4.3 RX5000



4.4 The Payment Flow – DX8000, RX5000 (ECR REST API and Stand-alone)

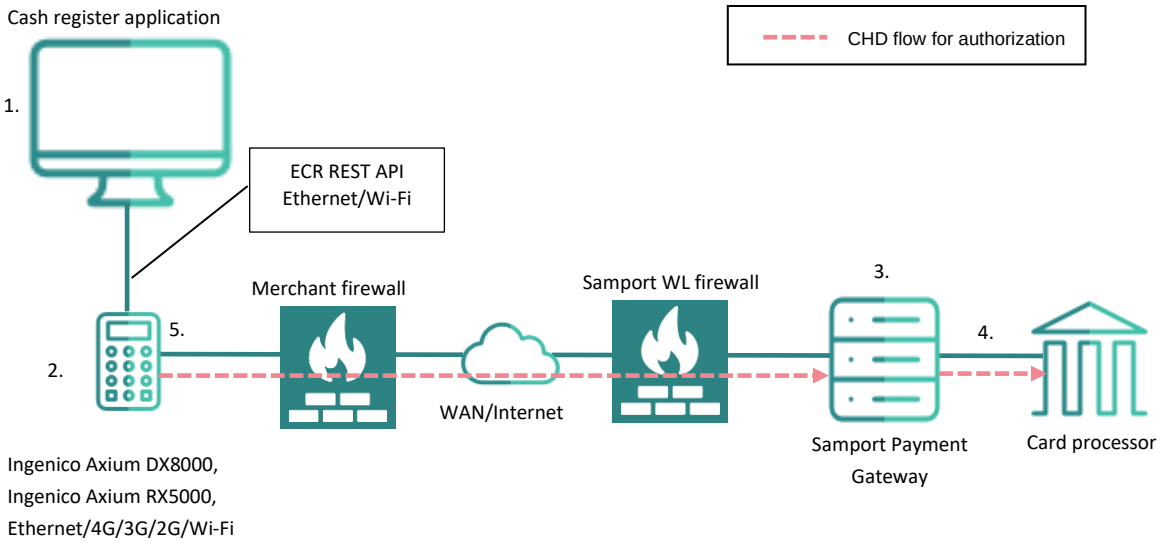


Diagram 1-1 the payment flow

1. If the terminal is integrated, the cashier selects payment from the ECR connected cash register. The cash register application contacts the terminal through HTTP.

2. When the terminal is used standalone, the transaction is initiated directly on the terminal. The cardholder will either swipe, insert or tap the card. Alternative, the card holder will enter the PAN, expire date and CVV2 (if required) in the terminal PED. The terminal will start to process the transaction. The cash register may request dialogs from the terminal to mirror the terminal display, if implemented. Ingenico's SRED-module OnGuard will encrypt (with DUKPT 256-bit key AES cipher) the cardholder data (CHD) and sensitive authentication data (SAD). When the payment application has all the information it needs for authorization, it will contact Samport payment gateway.

3. The terminal will connect to the gateway and send the encrypted transaction, using mTLS, for authorization.

4. The Samport payment gateway authorizes the payment request from the terminal against card processors and the result from the authorization will be processed and returned to the terminal. The result sent to the terminal contains no CHD nor SAD.

5. The payment application in the terminal holds the service code and expiration date in RAM. All other CHD/SAD is encrypted and also held in RAM. The data in RAM is purged when the transaction is processed or the terminal times out.

   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)

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

4.5 Requirements

The payment application is intended to be installed and used on Bambora Device POI models:
-DX8000 with PCI PTS approval number 4-30443. Please see PCI PTS approval number for valid firmware version: 4-30443.
-RX5000 with PCI PTS approval number 4-30527. Please see PCI PTS approval number for valid firmware version: 4-30527.

Used firmware version is found in the terminal menu: About > Terminal

4.6 Stand-Alone

4.6.1 Hardware Requirement

- Ingenico DX8000
  To use Wi-Fi, please activate in the terminal menu: Settings > Network settings > Wi-Fi.
  The DX8000 is delivered with a sim card. To activate or deactivate mobile connectivity please open terminal menu: Settings > Network settings > Mobile network. Make sure to activate Mobile data and Roaming.

Configurations:	Products:	Details:
Standalone Wireless Wi-Fi / Mobile Network	Terminal: DX8000 Config: Wi-Fi or/and Mobile connection 4G/3G/2G Charger base USB A to USB C straight 2,5m + USB A power adapter	Onomondo sim card

4.6.2 Software Requirement

- Bambora Device AB application Samport AX 1.5.0

4.7 Integrated

4.7.1 Hardware Requirement

- DX8000 and RX5000
  To be able to connect the terminal to a cash register application please activate Wi-Fi in the terminal menu. Settings > Network settings > Wi-Fi
  The RX5000 can alternatively use Ethernet. Activate at: Settings > Network settings > Ethernet

Configurations:	Products:
Integrated Wireless Wi-Fi	Terminal: DX8000 Config: Wi-Fi Charger base USB A to USB C straight 2,5m + USB A power adapter
Integrated Wired Ethernet or Integrated Wi-Fi	Terminal: RX5000 Config: Ethernet and/or Wi-Fi Direct HDMI to Ethernet 4m Power supply

4.7.2 Software Requirement

- Bambora Device AB application Samport AX 1.5.0
- Required TCP/IP port number: 8080
- Cash register with the following option (DX8000, RX5000)
  - PC Cash register application with ECR REST API support

4.8 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. 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:

Domain / IP	Protocol
*.samport.com	HTTPS
2.android.pool.ntp.org	NTP
www.google.com	HTTP, HTTPS
connectivitycheck.gstatic.com	HTTP
play.googleapis.com	HTTP
www.googleapis.cn	HTTP
developer.google.cn	HTTP
axyun.ingenico-axcloud.net	HTTPS, port 8100 and 8101
axyun.ingenico-axcloud.net	HTTP, port 81
firmwareota.unimarspay.com	HTTP
47.107.21.255	HTTP, port 1900
*.izatcloud.net	HTTPS
time.xtracloud.net	NTP
xtratime.qcomgeo2.com	NTP
slm-portal.icloud.ingenico.com	HTTPS

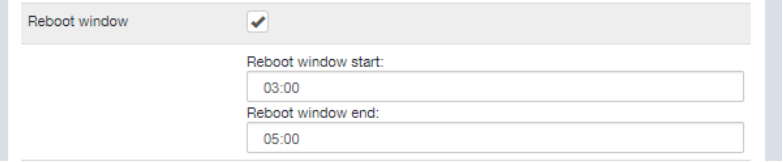
If no port is specified, use standard ports. (80 for HTTP, 443 for HTTPS and 123 for NTP.)

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

4.9 24h PCI reboot

The terminals have a mandatory daily reset mechanism introduced in PCI PTS v4. This reset can't be deactivated. The terminals will restart every 24h – 5 minutes. It means the terminals will restart 5 minutes earlier every day. Default setting is between 3:00 – 05:00.

E.g. terminal Tmin=03:00h Tmax=05:00h



Day 1: Terminal restarts at Tmax – 5 minutes.
Day 2: Terminal restarts at Tmax – 10 minutes.
When terminal reaches Tmin, the terminal restarts at Tmin AND Tmax.

Implementation

The ECR REST API is designed to be easy to use and integrate and provides a standardized way for applications to communicate with the AXIUM 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 cash register vendor needs to implement a client application in order to establish the connection. The Swagger specification describes implementation of the ECR REST API. Please contact the Integration Specialists to receive the Swagger and related integration questions such as hash calculation and secret key. See chapter Support for contact details.

Application Versioning Methodology

Samport AX is using Semantic Versioning system. https://semver.org/ Semantic Versioning is conveying information about changes, by 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			

Secure Software Updates

The Samport AX application receives updates from TMS through secure channel (TLS 1.2), the integrity of the files and parameters is supported by the terminal firmware.

Software is signed using Ingenicos SignKit and is validated by the firmware on the terminal. Parameter files are signed by the TMS with a private key and is validated by the firmware using a public key. No user interaction is allowed.

7.1.1 Application updates from TMS

The Samport AX payment application is distributed to the terminal in a secure manner. The terminal retrieves the software from Samport TMS using HTTPS and the connection is secured using TLS 1.2 (mutual authentication) 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.

Samport AX payment application does not provide any separate prompt files. (PCI SSF control objective B.5.1.5.)

The terminals do not rely on any other services or third-party software that need to be installed. (PCI SSF control objective 12.1.)

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

The payment application checks for automatic software updates at least once a day, (not in association with financial transactions). The download is not visible to the user. The software installation will take place at upstart for example after the 24h PCI reboot. The automatic update is handled by Bambora Device centrally.

If you want to check or request an update on the terminal manually, please follow these steps on the terminal:

1. Open the terminal menu 
2. Press Software update
3. Please allow time for the terminal to download the software
4. Press Install in the terminal menu

We strongly encouraged to update, as soon as possible, to the latest software versions available!
If there are any questions please contact our support, the contact details can be found in chapter Support.

The software version can be validated via terminal menu: About > Terminal

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 guidance 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.

Security Usage

The DX8000 and RX5000 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 will 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 Samport AX application. The application does not store any card validation codes, magnetic stripe data, PINS 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 encrypted SAD after the transaction has been processed. For offline transactions PAN and expiry date is stored encrypted with 256-bit DUKPT AES 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. The deletion process is not configurable by end user and does not require any user involvement, as it is provided by the modules within the terminal firmware.

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

No guidance for deleting card data is needed for either the terminal or cash register. The payment application never send SAD to the ECR. Regarding CHD, only truncated PAN is sent to the ECR for printing purposes. The terminal deletes encrypted card data that is stored on the restricted internal memory when an online transaction is sent to Bambora Device or as soon as the terminal gets connection.

The payment application does not retain Sensitive authentication data and clear PAN, and does not transmit or send the PAN in clear format through any of its interfaces:

- The sensitive authentication data is encrypted immediately at the time of the entry and never stored in the application. It is sent to the payment gateway through secure channel (TLS 1.2).
- Truncated PAN is printed and displayed masked in the ECR.
- 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 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:
The SRED Ingenico firmware OnGuard handles all the encryption of card holder data, not reachable from outside the terminal. The transaction data and the PIN block is encrypted with DUKPT 256-bit key AES cipher.

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. In all versions for the Samport AX application the card holder data is encrypted with a unique key per transaction. 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, 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 as this is a pre-defined function supported by the PCI PTS terminal.

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 Samport AX and the terminal database does not 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 and the application uses POI firmware functions for digital signature functions. 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 Bambora 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.
- 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.

Communication between terminal and cash register: Ethernet or Wi-Fi.

No other communication method is allowed. The Samport AX 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 Samport AX application does not store any cardholder data after an authorization. All authorizations are encrypted with AES DUKPT. Only encrypted PAN and expire date is stored (encrypted with AES DUKPT), on the terminals secure restricted internal memory, for offline transactions until they are sent to the Samport payment gateway. Once the terminal has received 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 Bambora 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 Bambora Worldline support immediately and report this, the contact details can be found in chapter 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 Sensitive data is secured during transmission.

Resellers and merchants applicability:
The Ingenico SRED module OnGuard handles all the encryption of cardholder data. The transaction data and PIN block are encrypted with AES using a DUKPT key (256-bit). The terminal communicates with the Samport Payment Gateway at the Bambora Device PCI DSS compliant environment through TLS 1.2 (mutual authentication). The Samport Payment Gateway is the only unit that can decrypt the data from the terminal and vice versa.

9.16 Use of multi-factor authentication

Resellers and merchants applicability:
The Samport AX application cannot be access 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.

9.17 Use of Cryptography

Resellers and merchants applicability:
PCI Secure Software Standard requirement 6 and 7. The Samport AX 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 Bambora Worldline for destruction. Please contact our support (contact details can be found in chapter 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 terminal runs out of unique DUKPT keys, the terminal must be replaced. The symptom is that all transactions are declined. DUKPT uses a 32 bit transaction counter where at most 16 bits can be 1, which yields more than one billion unique keys. If a terminal makes 1000 transactions per day, its estimated lifespan is more than one million days, or over 2700 years. If a terminal makes 10,000 transactions per day, its estimated lifespan is over 270 years.

9.18 PIN shield

Resellers and merchants applicability:
DX8000 is a handheld device without privacy shield. The RX5000 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 the DX8000 terminal in intended manner, handheld by the cardholder when entering PIN.

9.19 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.

9.20 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 at transaction request. The payment application has the right to reject transactions until the configuration files are updated to ensure the device remains up to date. Therefore, it's important to ensure that the payment terminal is allowed access to the requirements in this section: Network & Services Requirement

Extracts from PCI SSF 1.2 requirements:
9.1.a …to confirm that methods are implemented to validate the integrity of software executables and any configuration options, files, and datasets that the software relies upon for operation such that unauthorized post-deployment changes are detected.

9.21 Secure Defaults

Worldline 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 Samport AX application does not provide users with accounts or access. Vulnerabilities related to authentication and access are not relevant to the application.