Verifone®

PCI PA-DSS Implementation Guide

For Atos Worldline XENTEO ECO and YOMANI XR, Yomani terminals using the Payment Core BKX version A06.01.xxx

Version 3.01

Date: **24-Feb-2016**

Revision History

Version	Name	Date	Comments
1.00	Mats Oscarsson	2011-03-25	Initial revision
1.01	Mats Oscarsson	2011-06-10	Front page changed to cover the Yomani
1.02	Mats Oscarsson	2011-06-13	Chapter 3.4: Added information that the TMS used for PED SW distribution should be checked by a QSA. Chapters 2.1 and 3.4: Added instruction not to place the terminal in an Internet accessible network zone (“DMZ”).
2.01	Mats Oscarsson	2011-10-19	Updated for PCI PA-DSS version 2.0 Chapter “3.3 Protect Wireless Transmissions” is updated. Chapter “2.1 Build and Maintain a Secure Network, Requirement 1, c. What this means to you” is updated to describe the ports that need to be opened. Chapter “2.5 Regularly Monitor and Test Networks, Requirement 10, c. What this means to you” is updated to contain information about how to change to address to the centralized log server”
2.02	Mats Oscarsson	2012-10-01	Annual review. No change.
2.03	Mats Oscarsson	2013-07-08	Updated to cover the Xenoa Eco terminal
2.04	Mats Oscarsson	2013-10-01	Graphical layout changed Front page updated to cover both version A05.01 and A05.02.
2.05	Mats Oscarsson	2014-05-02	Front page changed to make a distinction between Yomani/Yomani XR and Xenteo/Xenteo ECO respectively.
3.00	Sergejs Melnikovs	2016-02-22	Document rebranding and update according to PCI DSS & PCI PA DSS version 3.1 requirements. Starting from this version the document covers only BKX Payment Core version A06.01.xxx
3.01	Aleksandrs Ivanovs	2016-02-24	Corrected menu options order in “5.1.How to change the address to the centralized log server”

References

Nbr.	Title	VERSION
1	Payment Card Industry – Payment Application Data Security Standard	3.1
2	Payment Card Industry – Data Security Standard	3.1

Table of Contents

1. Introduction

The Payment Card Industry Data Security Standard (PCI-DSS) defines a set of requirements for the configuration, operation, and security of payment card transactions in your business. If you use the Point BKX in your business to store, process, or transmit payment card information, this standard and this guide apply to you.

The requirements are designed for use by assessors conducting onsite reviews and for merchants who must validate compliance with the PCI DSS.

For more details about PCI DSS, please see the following link:

http://www.pcisecuritystandards.org

This guide is updated whenever there are changes in BKX software that affect PCI DSS and is also reviewed annually and updated as needed to reflect changes in the BKX as well as the PCI standards. Guidelines how to download the latest version of this document could be found on the following web site

http://www.verifone.se/

The Payment Card Industry (PCI) has also set the requirements for software applications that store, process or transmit cardholder data. These requirements are defined by the Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS). In order to facilitate for you to get a PCI DSS assessment the BKX Payment Core software has been validated by PCI to comply with the PCI PA-DSS requirements.

Note: This guide refers to Atos terminals using the BKX Payment Core. The version of the BKX Payment Core is listed on the PCI web site "List of Validated Payment Applications" that have been validated in accordance with PCI PA-DSS. If you cannot find the version of the BKX Payment Core running on your BKX application on that list please contact your helpdesk in order to upgrade your terminal.

http://www.pcisecuritystandards.org/

Document Use

This PA-DSS Implementation Guide contains information for proper use of the BKX application. Verifone Sweden does not possess the authority to state that a merchant may be deemed "PCI DSS Compliant" if information contained within this document is followed. Each merchant is responsible for creating a PCI DSS-compliant environment. The purpose of this guide is to provide the information needed during installation and operation of the BKX application in a manner that will support a merchant's PCI DSS compliance efforts.

Note 1: Both the System Installer and the controlling merchant must read this document. Hence, the Implementation Guide should be distributed to all relevant payment application users (customers, resellers and integrators)

Note 2: This document must also be used when training integrators/resellers at initial workshops.

2. Summary of PCI DSS requirements

This summary provides a basic overview of the PCI DSS requirements and how they apply to your business and the BKX terminal.

2.1. Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

a. What the requirement says

"Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network. Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.", reference 2.

b. How your BKX helps you meet this requirement

BKX is designed to operate in a network behind a firewall.

c. What this means to you

If you are using wireless technology you must install and maintain a firewall to protect your Point BKX from someone hacking the wireless environment. Also, if your network connection allows inbound traffic you should use a firewall. The terminal should not be placed in an Internet accessible network zone ("DMZ").

In case a firewall is connected between the terminal and the ECR/vending machine TCP port 2000 must be opened to enable communication between the two.
Port 2000 is used as default, but there is exist possibility to change port to which is more preferable. Changing port is performing via user menu (password protected) or via configuration file (PPL download).

For ports used for outbound traffic please refer to the information menu of the terminal.

1. Press the menu button on the terminal.
2. Enter password followed by the green button.
3. Select "3. INFORMATION"
4. Select "3. HOST INFO"
5. Now, by scrolling with using the green button, the ports used for outbound traffic are shown in the display.

For ECR type of communication (Ethernet, RS232) please refer to the information menu of the terminal.

1. Press the menu button on the terminal.
2. Enter password followed by the green button.
3. Select ”2. KOMMUNIKATION”
4. Select “2 KASSAANSLUTNING” to see ECR communication type
5. Select “2 KASSAANSLUTNINGPORT” to see ECR port value
6. “2 KASSAANSLUTNINGPORT” is protected by unique password

For more information about setting up your firewall to work with BKX application, please refer to the manual supplied by your firewall vendor.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

a. What the requirement says

“Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.”, reference 2.
Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

b. How your BKX helps you meet this requirement

BKX does not allow users to access any card holder data or sensitive authentication data. The application also doesn’t facilitate any non-console administrative access to the network. IP addresses for processors, terminal management systems and software download servers are protected by unique passwords per terminal and these passwords are changed on a daily basis.

c. What this means to you

Since the password protection for the BKX application is handled entirely within the unit and no any non-console administrative access provided there is no need for you to take any action.

2.2. Protect Cardholder Data

Requirement 3: Protect stored cardholder data

a. What the requirement says

“Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

Please refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for definitions of “strong cryptography” and other PCI DSS terms.”, reference 2.

b. How your BKX helps you meet this requirement

BKX application never stores full magnetic stripe data from the card. For offline transactions PAN and expiry date are stored encrypted using a unique key per transaction. The file is deleted once all content is sent and confirmed by host.

BKX application never displays full PAN of the card on the screen (except manual PAN entry dialogue). Full list of instances where PAN could be output to store outside of the application control represented in "Appendix C".

At transaction time PAN is truncated before it is stored, only the first 6 and last 4 digits are stored or encrypted full PAN. For printout of receipts and reports the truncated PAN is sent to the ECR.

c. What this means to you

For cards read by the BKX terminal magnetic stripe reader or chip card reader you do not have to take any action.

For manually entered PAN and for voice referrals it is never allowed to write down or otherwise store PAN, expiration date or CVV2.

If you store (as needed for business) cardholder data please don't use a public-facing systems (for example, web server and database server must not be on same server).

Do not utilize end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.) to send unprotected PAN unless they are configured to provide strong encryption.

Note: Sending of unprotected PANs via end-user messaging technologies strictly prohibited.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

a. What the requirement says

"Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.", reference 2.

b. How your BKX helps you meet this requirement

The BKX application encrypts card holder data using triple DES with a unique key per transaction. On top of that the entire messages sent to and from the BKX are protected using SSL/TLS, if the processor supports SSL/TLS protocol.

c. What this means to you

If you are using a wireless network, WLAN, you must set up your wireless network to use WPA/WPA2 encryption for new installations. **N.B. WEP must not be used.** The WLAN encryption is applied on top of the triple DES encryption and SSL/TLS (if SSL/TLS is supported by the processor) implemented in the terminal.

If BKX terminal connected to an external network without using WLAN you do not need to take any action.

2.3. Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

a. What the requirement says

Malicious software, commonly referred to as "malware" — including viruses, worms, and Trojans — enters the network during many business-approved activities including employee e-mail and use of

the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place, reference 2.

b. How your BKX helps you meet this requirement

The BKX cannot be used for e-mails or internet activities. All software downloaded to the terminal is controlled by Point, protected by a digital signature (MAC) and sent over an SSL/TLS connection (if the processor supports SSL/TLS). These security measures prevent malicious software being installed onto your BKX terminal.

c. What this means to you

You should install and maintain antivirus software which helps to protect your system. Make sure that this software is up to date as security threats change.

For the BKX you do not need to take any action regarding antivirus software.

Requirement 6: Develop and maintain secure systems and applications

a. What the requirement says

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.
Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques, reference 2.

b. How your BKX helps you meet this requirement

Verifone Sweden constantly works with the latest security findings and requirements throughout the life cycle of your BKX terminal. This includes automatic SW updates whenever necessary.

c. What this means to you

You should keep your system up to date with software updates, operating system updates, and any other security patches.

For the BKX terminal you do not need to take any action.

2.4. Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

a. What the requirement says

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to

know“ is when access rights are granted to only the least amount of data and privileges needed to perform a job, reference 2.

b. How your BKX helps you meet this requirement

The BKX application does not disclose any cardholder data. Sensitive authentication data is always encrypted when sent for authorization and never stored. PAN is always truncated and/or encrypted when stored, thus only truncated and/or encrypted PANs are sent to the ECR for printouts of reports, logs or receipts.

c. What this means to you

In case you need to enter card numbers manually or if you have to do voice referrals you must never keep written copies or otherwise store copies of cardholder data. Also, you must never e-mail, fax etc card holder data.

For cards read by the BKX terminal magnetic stripe reader or chip card reader you do not need to take any additional security measures.

Requirement 8: Identify and authenticate access to system components

a. What the requirement says

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system — particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage, reference 2.

b. How your Point BKX helps you meet this requirement

The BKX application does not allow access to critical data.

Requirement 8.3: The BKX application does not allow direct remote access to the system. But for remote updates via Terminal Management Systems the authentication used as part of an authenticated remote software distribution framework for the PED, should be evaluated by a QSA as part of any PCI DSS assessment.

c. What this means to you

Since the BKX does not allow access to critical data you do not need to take any action.

Requirement 8.3: Ask your QSA to include the remote update process in the PCI DSS assessment.

Requirement 9: Restrict physical access to cardholder data

a. What the requirement says

“Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately

restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.”, reference 2.

b. How your BKX helps you meet this requirement

The BKX application physically prevents by encryption and truncation users to access cardholder data.

c. What this means to you

For your BKX you do not need to take any action.

2.5. Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

a. What the requirement says

"Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.", reference 2.

b. How your BKX helps you meet this requirement

The BKX application keeps a log for the 1000 latest transactions. This log contains truncated PANs. No cardholder data is accessible from the BKX.

The BKX also keeps an Audit Trail to track changes to system level objects.

c. What this means to you

For the transaction log you do not need to take any action since no cardholder data is accessible.

For the Audit Trail there are no settings you need to do. The Audit Trail is created automatically and cannot be disabled. The Audit Trail could be sent manually to a centralized server by entering the BKX "LOG MENU", for further details please refer to the user's manual.

The address to the centralized log server is already set when you receive the terminal and normally there is no need to change that address in the terminal. However, if for some reason this address needs to be changed please contact the representative of your service provider. Chapter "5 Audit Trail log" also gives you guidance on how to change the address of the centralized log server.

Requirement 11: Regularly test security systems and processes

a. What the requirement says

"Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.", reference 2.

b. How your Point BKX helps you meet this requirement

Your BKX has mechanisms to ensure that software and parameters can be downloaded from trusted sources only. These mechanisms are based on cryptographic signatures and MAC protection (Message Authentication Code).

c. What this means to you

You should test your network connections (including wireless networks) periodically for vulnerabilities, and make use of network vulnerability scans. If you make any significant changes to your network, you should also test for vulnerabilities.

2.6. Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors

a. What the requirement says

"All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.", reference 2.

b. How your BKX helps you meet this requirement

----

c. What this means to you

----

3. How to set up your BKX terminal to ensure PCI DSS compliance

3.1. Do not retain full magnetic stripe or card validation code

When upgrading the payment application in your BKX terminal to comply with the PCI PA-DSS requirements this could be done two ways.

1. Your old unit is physically replaced by a new BKX loaded with software that complies with the PCI PA-DSS requirements. Since the old unit also contains PA DSS validated application there is no any historical sensitive authentication data stored on the unit. BKX application starting from version A04.27 are PCI PA DSS compliant.
2. Your existing BKX is downloaded remotely with new software that also complies with the PCI PA-DSS requirement.

In both cases you must make sure that the software version of the BKX Payment Core that runs on your BKX terminal is listed on the PCI web site “List of Validated Payment Applications” that have been validated in accordance with PCI PA-DSS.

http://www.pcisecuritystandards.org

In order for your organization to comply with PCI DSS requirements it is absolutely necessary to remove historical data stored prior to installing your PCI PA-DSS compliant BKX terminal. Therefore you must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) are removed from all storage devices used in your system, ECRs, PCs, servers etc. For further details please refer to your vendor.

No specific setup of your BKX PCI PA-DSS compliant terminal is required. PAN is stored either truncated or encrypted. Full magnetic stripe data and CVV2 is deleted immediately after authorization and never stored.

However, if you need to enter PAN, expiration date and CVV2 manually or do a voice referral you should never write down or otherwise store PAN, expiration date or CVV2. Collect this type of data only when absolutely necessary to perform manual entry or voice referral.

Note: Using the PCI PA-DSS compliant BKX terminal you will never be prompted to enter CVV2.

No any sensitive authentication data are retrieving by BKX application (even when needed to solve a specific problem) in production terminals. In case when sensitive authentication data need to be present in the logs for troubleshooting is only done at Verifone lab/test environment using test terminals.

3.2. Protect stored card holder data

PAN and expiration date are encrypted and stored in your BKX terminal for offline transactions. For this encryption a unique key per transaction is used. Once your BKX terminal goes online any stored transactions are sent to the processor and securely deleted from the BKX memory.

To comply with the PCI DSS requirements all cryptographic material must be rendered irretrievable. The removal of this material is handled within the BKX terminal and you do not need to take any action.

3.3. Protect wireless transmissions

If you are using wireless network within your business you must make sure that firewalls are installed that deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the BKX environment. Please refer to your firewall manual.

In case you are using a wireless network you must also make sure that:

- Encryption keys were changed from vendor defaults at installation.
- Encryption keys are changed anytime someone with knowledge of the keys leaves the company or changes position.
- Default SNMP community strings on wireless devices were changed
- Default passwords/passphrases on access points were changed
- Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks, for example IEEE 802.11i. Please note that the use if WEP as a security control was prohibited as of 30 June 2010.
- Other security related wireless vendor defaults were changed.

3.4. Facilitate secure remote software updates

The software of your BKX terminal could be updated remotely and automatically. For connection to external networks it is recommended to use firewall protection as per ”2.1 Build and Maintain a Secure Network” in this document. The terminal should not be placed in an Internet accessible network zone (“DMZ”).

Also the security part of the software that resides in the PED (PIN Entry Device) part of the terminal could be updated remotely. The Terminal Management System that is used for distribution of the PED software should be evaluated by a QSA as part of any PCI DSS assessment.

3.5. Encrypt sensitive traffic over public networks

Your BKX application allows transmission over public networks, e.g. public internet. To protect sensitive data your BKX application uses triple DES encryption with a unique key per transaction. On top of that all data sent to and from the BKX is protected under SSL/TLS, if the processor supports SSL/TLS. To connect your BKX application to public networks you do not need to take any further action regarding encryption.

4. Back-out or product de-installation procedures

The software of your BKX terminal could be updated remotely either automatically or manually triggered. In the unlikely event that your newly downloaded software fails or malfunctions please contact your TMS operator in order to allow you to download an older version of the software.

5. Audit Trail log

5.1. How to change the address to the centralized log server

By default the Audit Trail is sent to a centralized log server hosted by your PSP. If you want to continue to use that log server you don't have to take any action.

On Yomani XR / Xenteo ECO Solution:

1. Select "MENU"
2. Select (4) "CONFIGURATION"
3. Select (3) "HOST PARAMETERS"
4. Select (3) "ELOG" (for E,A,C,K log types)
5. Enter IP address
6. Enter port number

However, if you want to use another server and receive the Audit Trail in SYSLOG format then do as follows.

On Yomani XR / Xenteo ECO Solution:

7. Select "MENU"
8. Select "FUNKTIONER"
9. Scroll down to "LOGGMENY"
10. Select "A-LOG" (Audit Trail)
11. Select "SKICKA TCP SYSLOG"
12. Enter IP address for Syslog Server
13. Enter PORT number
14. Select "REAL-TIME SKICKA"

Once A-LOG in SYSLOG format is activated, all information of major events will be transferred to your designated server. Terminal will keep theses settings even after power loss or reboot.

Important:

- SysLog is sent in TCP message instead of UDP. Make sure your SysLog server supports it.
- SysLog is based on standard internet protocols as specified by RFC 3164 and RFC 3195.

5.2. Data Contents of Audit Trail

The format of the terminal log file needed to meet the PCI DSS requirement 10, "Track and monitor all access to network resources and cardholder data", described in PCI Requirements and Security Assessment Procedures Version 3..

5.2.1. File size

The size of the file has to be decided for each application/platform. According to PCI DSS requirement 10.7 audit trails must be retained for at least three months online (ready for immediate forensic analysis) and for a total of one year.

5.2.2. File format

The terminal audit log file should be a readable ASCII text file with one entry on each line. The log entries should consist of data according to table below with each value separated by semi-colon ";" last data element is also padded with ';' character. This makes it possible to import the file to a number of existing database programs.

Requirement	Name	Value
10.3.1	User ID	Full name of process or script depending on application/platform.
10.3.2	Type of event	See table below
10.3.3	Date & Time	YYMMDDhhmmss
10.3.4	Success	OK / NOK
10.3.5	Origination	Auto / Man / Timer
10.3.6	Content data	Depending on type of event. See table below. In case of several data entries in single event separator "!" is used to split data entries.
	Trailer	Newline characters indicating end of log entry: '\n' (0x0A)

SysLog is sent in TCP message instead of UDP. Make sure your SysLog server supports it.
SysLog is based on standard internet protocols as specified by RFC 3164 and RFC 3195.

Event Type	Content	Description
Download	file = [filename downloaded]([download location])	Result of file download from remote host. Indicates file name downloaded and ip+port of remote host from which file was downloaded
Validate	file = [filename validated]	Validation result of file
Install	file = [filename installed]	Installation result of file
Configuration	[parameter name] old = [Old paramete value] new = [New parameter value]	Terminal configuration change affecting host IP configuration, terminal Identifiers, rescheduling of operations, change of terminal identifiers or user password change.
Audit send	ip:port = [destination ip:port]	Result of audit log sending. Indicates destination server which the log was sent to.
RT Audit Start	ip:port = [syslog server ip:port]	Start of Real-Time audit log sending to SysLog server. Indicates IP&Port of destination syslog server.
RT Audit Stop	reason = [reason for stop]	Interruption of Real-Type audit log sending to syslog server. Optionally indicates reason for stopping: e.g. technical failure, customer interruption, etc.
Startup	Audit log started – A-LOG STARTED TERM.TYPE: [value] APP.VERS: [value] MILESTONE: [value] BUILD: [value] Paymentcore: [value] Key version: [value] samoa version: [value] SHA1: [value] /mp1.img SHA1: [value] /linux SHA1: [value] /pfrEMV/EmvEng SHA1: [value] /EmvEng MD5: [value] /ePoint MD5: [value] /ppEng MD5: [value] /pwEng	Indicates application startup. Indicates application version as well as versions and checksums of external modules.

5.2.3. File format

Below is an example of log entries from a terminal:

```
pfaMAIN;Audit send;20151222142218;NOK;Man  ;FAILED TO SEND AUDIT LOGS
pfaMAIN;Config    ;20151222142218;OK ;Auto ;[ELOG]IsSent old=0!new=1
pfrPPM ;Download  ;20160212080434;OK ;Man  ;file=CTLSPAR_160212070411
pfrPPM ;Config    ;20160212080434;OK ;Auto ;[PPM]RecoverFile
old=CTLSPAR_160212070411!new=CTLSPARH16
pfrPPM ;Download  ;20160212080435;OK ;Man  ;file=CTLSPARH160212070411
pfrPPM ;Validate  ;20160212080436;OK ;Man  ;file=MASPAR__160212070408
pfrPPM ;Replaced  ;20160212080439;OK ;Man  ;file=DCPAR___160211132821
pfrPPM ;Install   ;20160212080439;OK ;Man  ;file=DCPAR___160212070408
pfrPPM ;Replaced  ;20160212080441;OK ;Man  ;file=BINPAR__160211132822
pfrPPM ;Install   ;20160212080441;OK ;Man  ;file=BINPAR__160212070410
pfrPPM ;Replaced  ;20160212080441;OK ;Man  ;file=CTLSPAR_160211132851
pfrPPM ;Install   ;20160212080441;OK ;Man  ;file=CTLSPAR_160212070411
pfrPPM ;Replaced  ;20160212080442;OK ;Man  ;file=CTLSPARH160211132852
pfrPPM ;Install   ;20160212080442;OK ;Man  ;file=CTLSPARH160212070411
pfaMAIN;Config    ;20160212081005;OK ;Auto ;[PPM]DoLogon old=1!new=0
pfaMAIN;Config    ;20160212081006;OK ;Auto ;[PPM]TriggerTime
old=000000000000!new=160213045800
pfaMAIN;Config    ;20160212081006;OK ;Auto ;[AUTH]HandlingCode
old=224!new=225
pfrSPDH;Config    ;20160212081700;OK ;Auto ;[SSL]HostSPDHToday old=1!new=2
pfrSPDH;Config    ;20160212082315;OK ;Auto ;[SSL]HostSPDHToday old=2!new=1
pfrPPM ;Validate  ;20160122105928;OK ;Man  ;file=MASPAR__160122093708
pfrPPM ;Validate  ;20160122105928;OK ;Man  ;file=DCPAR___160122093709
pfrPPM ;Validate  ;20160122105928;OK ;Man  ;file=BINPAR__160122093710
pfrPPM ;Validate  ;20160122105931;OK ;Man  ;file=CAPUB___130320115017
```

6. Terminology and abbreviations

BKX Application	Payment Application with BKX as a payment core
BKX Terminal	Terminal with installed BKX Application
Cardholder Data	PAN, Expiration Date, Cardholder Name (not used by Point BKX) and Service Code.
CVV2	Card Verification Value, also called CVC2, is a three or four digit value printed on the back of the card but not encoded on the magnetic stripe or the chip.
ECR	Electronic Cash Register
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a combination of the Hypertext Transfer Protocol with the SSL protocol to provide encrypted communication and secure identification.
Magnetic Stripe Data	Track data read from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.
PAN	Primary Account Number. PAN, also called card number, is part of the magnetic stripe data and is also printed or embossed on the card. PAN can also be stored in the chip of the card.
PCI DSS	Payment Card Industry Data Security Standard, the subject of this document. Retailers that use applications to store, process or transmit payment card data are subject to the PCI DSS standard.
PCI PA-DSS	Payment Card Industry Payment Application Data Security Standard is a standard for validation of payment applications that store, process or transmit payment card data. Applications that comply with PA DSS have built in protection of card data and hereby facilitates for retailers to comply with PCI DSS.
PED	PIN Entry Device.
PIN	Personal Identification Number. Secret numeric password known only to the user and a system to authenticate the user to the system.
PSP	Payment Service Provider offers merchants online services for accepting electronic payments.
Sensitive Authentication Data	Magnetic Stripe Data, CVV2 and PIN.
Service Code	A three digit code from the magnetic stripe data defining (1) Interchange and technology, (2) Authorization processing and (3) Range of services and PIN requirements.
SNMP	Simple Network Management Protocol, is a network protocol. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
SSH	Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices.
SSL	Secure Sockets Layer is a commonly used method to protect transmission across public networks. SSL includes strong encryption.
SYSLOG	Syslog is a standard for computer data logging.
TCP	Transmission Control Protocol is one of the core protocols of the Internet protocol suite.
TLS	Acronym for “Transport Layer Security.” Designed with goal of providing data secrecy and data integrity between two communicating applications. TLS is successor of SSL.
TMS	Terminal Management System.
UDP	User Datagram Protocol is one of the core protocols of the Internet protocol suite.
WEP	Wired Equivalent Privacy, a wireless network security standard. Sometimes erroneously called "Wireless Encryption Protocol"
WPA and **WPA2**	Wi-Fi Protected Access, is a certification program created by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks.

Appendix A: BKX Version Numbering Policy

Version number consists of 4 elements. Non-static elements are separated by '.' (dot) symbol.

The format is Axx.yy.zzz where

- **A**: Static letter, does not change.

- **xx**: Major version (numeric values 01-99) Initial value is 01 The value is never reset within application lifecycle.

The major version number is incremented in case of major changes to payment process, change that impacts security functionality. Requires a full PA-DSS assessment.

- **yy**: Minor version: (numeric values 01-99) Initial value is 01. The value is reset to '01' if major version number is changed.

The minor version number is incremented in case of large feature additions, terminal model additions, any cause of delta-assessment, partial audit, re-audit due to expiration etc.

- **zzz**: Wildcard / Revision. (numeric values 001 – 999). Initial value is 001. The value is reset if minor or major version number is changed.

Revision number is incremented in case of minor change which has impact on the application functionality but no impact on security or PA-DSS Requirements.

Appendix B: BKX Terminal files

In table below represented list of files on the terminal what can contains any cardholder data

File Name	Description	Cardholders data	Protection
SnFLog.tbl **SnFLog.tbl~**	Transaction information pending to be sent to Authorization host	PAN, Expiry Date	Encrypted by DUKPT
pfaMAIN.log	pfaMAIN activity trace.	PAN	Masked (6 first + 4 last)
pfrLPP.log	pfrLPP activity trace. Contain transaction result which should be send to ECR.	PAN	Masked (6 first + 4 last)
snftxn.txt	Temporary file for stored transaction logs	PAN, Expiry Date	Encrypted by DUKPT
TxnLog.tbl **TxnLog.tbl~**	Transaction log data. Used for printing report of last transactions. Stores last 1000 transaction data as maximum.	PAN	Masked (6 first + 4 last)

Appendix C: Instances where PAN is displayed

Instance	Description	Protection
DISPLAY	Only during manual PAN entry dialogue.	none
Transaction Result Message to ECR	Receipt data. ECR is responsible for cardholders receipt printing on the paper.	Masked (6 first + 4 last) and/or Encrypted full PAN