Verifone

PCI PA-DSS Implementation Guide

PBMUECR 04.21.004.xxxxx

Version 1.0(Release)

Date: **2019-10-23**

Contents

Contents 2
1. Introduction 3
1.1 Purpose 3
1.2 Document Use 3
1.3 References 4
1.4 Update History 4
1.5 Terminology and abbreviations 5
2 SUMMARY OF PCI DSS REQUIREMENTS 6
2.1 PA-DSS Req. 1.1.4: Historical data deletion 6
2.2 PA-DSS Req. 1.1.5: Securely delete any sensitive data used for debugging or troubleshooting 6
2.3 PA-DSS Req. 2.1: Purging cardholder data 6
2.4 PA-DSS Req. 2.2: Mask PAN when displayed 7
2.5 PA-DSS Req. 2.3: Render PAN unreadable anywhere it is stored 7
2.6 PA-DSS Req. 2.4: Protect keys 7
2.7 PA-DSS Req. 2.5: Implement key management processes and procedures 7
2.8 PA-DSS Req. 2.6: Provide a mechanism to render irretrievable any cryptographic key material 8
2.9 PA-DSS Req. 3.1: Unique user IDs and secure authentication 8
2.10 PA-DSS Req. 3.2: Unique user IDs and secure authentication for access to servers etc. 8
2.11 PA-DSS Req. 4.1: Implement automated audit trails 9
2.12 PA-DSS Req. 4.4: Facilitate centralized logging 9
2.13 PA-DSS Req. 5.4.4: Application versioning methodology 9
2.14 PA-DSS Req. 6.1: Securely implement wireless technology 9
2.15 PA-DSS Req. 6.2: Secure transmission of cardholder data over wireless networks 10
2.16 PA-DSS Req. 6.3: Provide instructions for secure use of wireless technology 10
2.17 PA-DSS Req. 7.2.3: Instructions for customers about secure installation and updates 11
2.18 PA-DSS Req. 8.2: Must only use secure services, protocols and other components 11
2.19 PA-DSS Req. 9.1: Store cardholder data only on servers not connected to the Internet 11
2.20 PA-DSS Req. 10.1: Implement two-factor authentication for remote access to payment application 12
2.21 PA-DSS Req. 10.2.1: Securely deliver remote payment application updates 12
2.22 PA-DSS Req. 10.2.3: Securely implement remote access software 12
2.23 PA-DSS Req. 11.1: Secure transmissions of cardholder data over public networks 12
2.24 PA-DSS Req. 11.2: Encrypt cardholder data sent over end-user messaging technologies 13
2.25 PA-DSS Req. 12.1, 12.1.1 and 12.2: Secure all non-console administrative access 13
Annexes 14
A1 Terminal files 14
A2 Application Version Numbering policy 14
A3 Instances where PAN is displayed 15
A4 Application components and used protocols 15

1. Introduction

1.1 Purpose

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 Verifone PBMUECR merchant unit application 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.

Failure to comply with these standards can result in significant fines if a security breach should occur. For more details about PCI DSS, please see the following link:

http://www.pcisecuritystandards.org

This guide is updated whenever there are changes in PBMUECR software that affect PCI DSS and is also reviewed annually and updated as needed to reflect changes in the PBMUECR 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.lv/

The Payment Card Industry 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 Verifone software application has been approved by PCI to comply with the PCI PA-DSS requirements.

Note: This guide refers to PBMUECR software versions 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 your PBMUECR application on that list please contact our helpdesk at Verifone Baltic in order to upgrade your terminal.

http://www.pcisecuritystandards.org/

1.2 Document Use

This PA-DSS Implementation Guide contains information for proper use of the Verifone PBMUECR merchant unit application. Verifone Baltic SIA does not possess the authority to state that a merchant may be deemed "PCI Compliant" if information contained within this document is followed. Each merchant is responsible for creating a PCI-compliant environment. The purpose of this guide is to provide the information needed during installation and operation of the PBMUECR merchant unit 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 ECR integrators/resellers at initial workshops.

1.3 References

(1) *Payment Card Industry – Payment Application Data Security Standard v3.2*
(2) *Payment Card Industry – Data Security Standard v3.2*
(3) *Terminal Audit Log v1.7*
(4) *Verifone Baltic – Terminal Software Version Numbering Specification v1.4.1*

1.4 Update History

Ver.	Name	Date	Comments
1.0	Sergejs Melnikovs	2019-10-23	- IG release with guidance only for PBMUECR version 04.21.004.xxxxx application; - Updated list of supported PED applications; - Extended explanation about wireless communication supported by the applications

1.5 Terminology and abbreviations

3DES	Triple DES common name for the Triple Data Encryption Algorithm
AES	Advances encryption standard
Cardholder Data	PAN, Expiration Date, Cardholder Name and Service Code.
Security codes	F. ex. Card Verification Value, also called CVV2, is a three or four digit value printed on the back of the card but not encoded on the magnetic stripe or the chip. Supplying this code in a transaction is intended to verify that the card is present at the point of sale when PAN is entered manually or when a voice referral is performed.
ECR	Electronic Cash Register
HSM	Hardware security module
Magnetic Stripe Data	Track data read from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.
PBMUECR Application	Terminal Merchant Unit Application for use in Baltic States (Estonia, Latvia, Lithuania)
PBMUECR Terminal	Terminal with installed PBMUECR Application
PCI PA-DSS	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.
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. Retailers that use applications to store, process or transmit payment card data are subject to the PCI DSS standard.
PCI PTS	Payment Card Industry PIN Transaction Security
PED	PIN Entry Device
POS	Point of sale
Sensitive Authentication Data	Magnetic Stripe Data, Security Codes, PINs/PIN-block.
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.
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. In this document TLS refers on TLS version 1.2
TMS	Terminal management system
TRSM	Tamper resistant security module
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.

2 SUMMARY OF PCI DSS REQUIREMENTS

This summary provides basic overview of the PCI PA-DSS requirements that have a related to Implementation Guide topic. It also explains how the requirement is handled on the PBMUECR application side and required actions for your (as a customer).

The complete PCI DSS and PA-DSS documentation can be found at:

http://www.pcisecuritystandards.org

Note: If a Terminal Management Systems is used as part of an authenticated remote software distribution framework for the PED, it should be evaluated by a QSA as part of any PCI DSS assessment.

2.1 PA-DSS Req. 1.1.4: Historical data deletion

Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the payment application	
How PBMUECR application meets this requirement	No specific setup for PBMUECR application is required. New version of PBMUECR application does not use any cardholder's sensitive historical data collected by previous version of the application. On installation, PBMUECR application performs secure wipe for all terminal's memory, which is available for custom application files.
merchant/reseller actions required	You must make sure that historical data (magnetic stripe data, cardholder data and CVV2s) are removed from all other storage devices used in your systems, ECRs, PCs, servers etc. For further details please refer to your vendor. Removal of sensitive authentication data is absolutely necessary for PCI DSS compliance.

Aligns with PCI DSS Requirement 3.2

2.2 PA-DSS Req. 1.1.5: Securely delete any sensitive data used for debugging or troubleshooting

Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.	
How PBMUECR application meets this requirement	No any sensitive cardholder's data are retrieving by PBMUECR application in Verifone production terminals. In case when sensitive cardholder's data need to be present in the logs for troubleshooting is only done at Verifone lab/test environment using test terminals.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.2

2.3 PA-DSS Req. 2.1: Purging cardholder data

Securely delete cardholder data after customer-defined retention period.	
How PBMUECR application meets this requirement	PBMUECR application doesn't store any cardholder data. All cardholder data transmitted to PED over RS232 cable for payment processing on a PED device.
merchant/reseller actions required	If the terminal prints full PAN on merchant receipt, please securely protect the merchant receipts/data and securely delete them after retention period in accordance with PCI DSS Requirements. Such protection is absolutely necessary for PCI DSS compliance.

Aligns with PCI DSS Requirement 3.1

2.4 PA-DSS Req. 2.2: Mask PAN when displayed

Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed) so only personnel with a business need can see the full PAN.	
How PBMUECR application meets this requirement	Manual PAN entry input form is only the place where PAN is displayed. After PAN manual entered there is no any option to display the PAN on the screen of PBMUECR terminal, even masked first 6 last 4. Full list of instances where PAN could be shown, including but not limited to POS devices, screens, logs, and receipts are available in Annex *A3 Instances where PAN is displayed*. Receipt design and data what is printed on PBMUECR terminal received from pin pad with dependent MultiPOINT application.
merchant/reseller actions required	If the terminal prints full PAN on merchant receipt, please securely protect the receipts in accordance with PCI DSS Requirement 3.3 and ensure that the data available only to personnel with a legitimate business need can see the full PAN.

Aligns with PCI DSS Requirement 3.3

2.5 PA-DSS Req. 2.3: Render PAN unreadable anywhere it is stored

Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs). The PAN must be rendered unreadable anywhere it is stored, even outside the payment application (for example, log files output by the application for storage in the customer environment)	
How PBMUECR application meets this requirement	The application doesn't store cardholder data on PBMUECR terminal, even truncated (first 6 last 4) version. The application does not allow plaintext PAN output for debugging/ troubleshooting purpose.
merchant/reseller actions required	The customer is responsible for rendering PAN unreadable in all instances where a PAN could be stored in outside of PBMUECR application.

Aligns with PCI DSS Requirement 3.4

2.6 PA-DSS Req. 2.4: Protect keys

Protect keys used to secure cardholder data against disclosure and misuse. Access to keys used for cardholder data encryption must be restricted to the fewest possible number of key custodians. Keys should be stored securely.	
How PBMUECR application meets this requirement	PBMUECR application doesn't store any cardholder data. All cardholder data transmitted to PED over RS232 cable for payment processing on a PED device
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.5

2.7 PA-DSS Req. 2.5: Implement key management processes and procedures

Implement key-management processes and procedures for cryptographic keys used for encryption of cardholder data.	
How PBMUECR application meets this requirement	PBMUECR application doesn't store any cardholder data. All cardholder data transmitted to PED over RS232 cable for payment processing on a PED device
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.6

2.8 PA-DSS Req. 2.6: Provide a mechanism to render irretrievable any cryptographic key material

Provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.	
How PBMUECR application meets this requirement	PBMUECR application doesn't store any cardholder data. All cardholder data transmitted to PED over RS232 cable for payment processing on a PED device
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 3.6

2.9 PA-DSS Req. 3.1: Unique user IDs and secure authentication

Use unique user IDs and secure authentication for administrative access and access to cardholder data.	
How PBMUECR application meets this requirement	This requirement cannot be applied to the PBMUECR application because there is no user login for the application itself. It runs on a Hardware terminal without requiring an operator or admin login. All changes on PBMUECR terminal handled by PED application connected to PBMUECR over RS232 cable.
merchant/reseller actions required	All other systems in the cardholder data should be protected by PCI-compliant authentication methods. That means: - Each user account must be assigned a unique ID. - The authentication must be performed at least either by a password, a token, or some biometric. - No group accounts or generic accounts may be used. - User passwords must be changed every 90 days. - A password must be at least seven characters long. - The password must consist of numeric and alphabetic characters. - The password history must be saved and a password must be different from the last four passwords used. - The account must be locked after no more than six invalid login attempts. - A lock must last at least 30 seconds. - After 15 minutes of inactivity, the user must authenticate again. - Assigning secure authentication to all default accounts in use - Any default accounts which are not required must be disabled or removed.

Aligns with PCI DSS Requirement 8.1 and 8.2

2.10 PA-DSS Req. 3.2: Unique user IDs and secure authentication for access to servers etc.

Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.	
How PBMUECR application meets this requirement	PBMUECR application does not provide functionality and does not maintain user accounts for administrative access or individual access to cardholder data.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 8.1 and 8.2

2.11 PA-DSS Req. 4.1: Implement automated audit trails

Implement automated audit trails.	
How PBMUECR application meets this requirement	PBMUECR application has an Audit Trail logging functionality. The application does not log any cardholder data. The application keeps an Audit Trail to track changes to system level objects. Audit trail logging is enabled by default. Audit trail logging is not configurable from the payment application. Audit trail logging should not be disabled. If disabled – it could result in non-compliance in PCI DSS.
merchant/reseller actions required	The application uses syslog protocol for audit trails. If you need to receive this data on your syslog server too please follow description in *(3) Terminal Audit Log v1.7.*

Aligns with PCI DSS Requirement 10.1

2.12 PA-DSS Req. 4.4: Facilitate centralized logging

Facilitate centralized logging.	
How PBMUECR application meets this requirement	The PBMUECR application provides ability to collect/analyze logging information by sending log files to remote host. The log file has syslog format and described in separate document *(3) Terminal Audit Log v1.7*.
merchant/reseller actions required	The application uses syslog protocol for audit trails. If you need to receive this data on your syslog server too please follow description in *(3) Terminal Audit Log v1.7.*

Aligns with PCI DSS Requirement 10.5.3

2.13 PA-DSS Req. 5.4.4: Application versioning methodology

Implement and communicate application versioning methodology.	
How PBMUECR application meets this requirement	Detailed description of version numbering methodology available in Annex *A2 Application Version Numbering policy* of the implementation guide.
merchant/reseller actions required	The merchant/reseller needs to understand which version of the merchant unit application they are using, and ensure validated versions are in use.

2.14 PA-DSS Req. 6.1: Securely implement wireless technology

Securely implement wireless technology. For payment applications using wireless technology, the wireless technology must be implemented securely.	
How PBMUECR application meets this requirement	PBMUECR application is designed to operate only with PA-DSS validated PED applications. List of supported PED application available in chapter *A4 Application components and used protocols.* Wireless configuration for PBMUECR application managed by PED application.
merchant/reseller actions required	The merchant/reseller must validate payment application on attached PED device. List of supported payment applications (see chapter *A4 Application components and used protocols*) The merchant/reseller must follow implementation Guide of the payment application. If you are using wireless network within your business, you must make sure, that firewalls are installed, what deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the PBMUECR terminal. Please refer to your firewall manual.

Aligns with PCI DSS Requirements 1.2.3 & 2.1.1

2.15 PA-DSS Req. 6.2: Secure transmission of cardholder data over wireless networks

Secure transmissions of cardholder data over wireless networks. For payment applications using wireless technology, payment application must facilitate use of industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	
How PBMUECR application meets this requirement	PBMUECR application is designed to operate only with PA-DSS validated PED applications. List of supported PED application available in chapter *A4 Application components and used protocols.* Wireless configuration for PBMUECR application managed by PED application.
merchant/reseller actions required	The merchant/reseller must validate payment application on attached PED device. List of supported payment applications (see chapter *A4 Application components and used protocols*) The merchant/reseller must follow implementation Guide of the payment application.

Aligns with PCI DSS Requirement 4.1.1

2.16 PA-DSS Req. 6.3: Provide instructions for secure use of wireless technology

Provide instructions for secure use of wireless technology.	
How PBMUECR application meets this requirement	PBMUECR application is designed to operate only with PA-DSS validated PED applications. List of supported PED application available in chapter *A4 Application components and used protocols.* Wireless configuration for PBMUECR application managed by PED application.
merchant/reseller actions required	The merchant/reseller must validate payment application on attached PED device. List of supported payment applications (see chapter *A4 Application components and used protocols*) The merchant/reseller must follow implementation Guide of the payment application. If you are using wireless network within your business, you must make sure, that firewalls are installed, what deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into terminal payment application environment. Please follow instructions of 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 are changed • Firmware on wireless devices is updated to support strong encryption, WPA/WPA2. Please note that WEP must not be used for new installations and is not allowed after June 30, 2010 • Other security related vendor defaults are changed

Aligns with PCI DSS Requirements 1.2.3, 2.1.1, & 4.1.1

2.17 PA-DSS Req. 7.2.3: Instructions for customers about secure installation and updates

Provide instructions for customers about secure installation of patches and updates.	
How PBMUECR application meets this requirement	PBMUECR application facilitates secure update functionality by downloading updates directly from a management server over MultiPOINT application on the PED, verifying integrity and authenticity of the update through digital signatures and applying updates to the terminal when it's not in use. Once a security patch or update of PBMUECR application released by Verifone our Product Manager notifies by email (or via phone call) responsible person of the integrator/reseller and provides encrypted package by corresponding integrator/reseller's public PGP key, signs it with his own private PGP key and provides it to the integrator/reseller's contact person via email or other communication channel which is agree in advance with the integrator/reseller.
merchant/reseller actions required	The merchant is not required to take any action in relation to this requirement because MultiPOINT once per 24h connects to management server and downloads a new version of PBMUECR application if that command received from the server. After download completed, MultiPOINT application transfers new version of PBMUECR application to Merchant Unit over RS232 cable. The integrator/reseller which provides management server service to the customer should configure the management server to deliver patches and updates to terminal once it's received from Verifone according to PCI DSS required timeframe.

2.18 PA-DSS Req. 8.2: Must only use secure services, protocols and other components

Use only necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties.	
How PBMUECR application meets this requirement	PBMUECR application does not employ unnecessary or insecure services or functionality. Full list of application components and dependent components / protocols described in Annex *A4 Application components and used protocols*
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 2.2.3

2.19 PA-DSS Req. 9.1: Store cardholder data only on servers not connected to the Internet

Store cardholder data only on servers not connected to the Internet.	
How PBMUECR application meets this requirement	PBMUECR application does not store any cardholder data in a server connected to the internet.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 1.3.7

2.20 PA-DSS Req. 10.1: Implement two-factor authentication for remote access to payment application

Implement two-factor authentication for all remote access to payment application that originates from outside the customer environment.	
How PBMUECR application meets this requirement	PBMUECR application does not provide the functionality and does not maintain user accounts for any remote access to the application.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 8.3

2.21 PA-DSS Req. 10.2.1: Securely deliver remote payment application updates

Securely deliver remote payment application updates. If payment application updates are delivered via remote access into customers' systems, software vendors must tell customers to turn on remote-access technologies only when needed for downloads from vendor, and to turn off immediately after download completes. Alternatively, if delivered via VPN or other high-speed connection, software vendors must advise customers to properly configure a firewall or a personal firewall product to secure "always-on" connections	
How PBMUECR application meets this requirement	PBMUECR application facilitates secure update functionality by downloading updates directly from a management server over MultiPOINT application on the PED, verifying integrity and authenticity of the update through digital signatures and applying updates to the terminal when it's not in use. Connection to the management server initiated by the MultiPOINT payment application according to configuration.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirements 1 and 12.3.9

2.22 PA-DSS Req. 10.2.3: Securely implement remote access software

Securely implement remote-access software.	
How PBMUECR application meets this requirement	PBMUECR application does not provide remote access functionality and does not maintain user accounts for any remote access to the application.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirements 2, 8 and 10

2.23 PA-DSS Req. 11.1: Secure transmissions of cardholder data over public networks

Secure transmissions of cardholder data over public networks.	
How PBMUECR application meets this requirement	PBMUECR application does not initiate sending any cardholder data over public network. All manipulation with cardholder data is handled (encrypted/stored) by PED application connected to PBMUECR over RS232 cable. PBMUECR just retransmit IP packets (received from PED) to public network. In doing so, PBMUECR does not send rather facilitates sending.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 4.1

2.24 PA-DSS Req. 11.2: Encrypt cardholder data sent over end-user messaging technologies

Encrypt cardholder data sent over end-user messaging technologies. If the payment application facilitates sending of PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat), the payment application must provide a solution that renders the PAN unreadable or implements strong cryptography, or specify use of strong cryptography to encrypt the PANs.	
How PBMUECR application meets this requirement	PBMUECR application doesn't use any end-user messaging technologies to send cardholder data.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 4.2

2.25 PA-DSS Req. 12.1, 12.1.1 and 12.2: Secure all non-console administrative access

Encrypt non-console administrative access. Use multi-factor authentication for all personnel with non-console administrative access.	
How PBMUECR application meets this requirement	PBMUECR application does not provide non-console access functionality and does not maintain user accounts for any administrative access to the application.
merchant/reseller actions required	The merchant/reseller is not required to take any action in relation to this requirement.

Aligns with PCI DSS Requirement 2.3

Annexes

A1 Terminal files

In a table below represented list of files on the terminal what can contains any cardholder data or logs of important events from the terminal.

File Name	Description	Cardholders data	Protection
#DSS.LOG	Audit log	n/a	n/a

A2 Application Version Numbering policy

Below represented PBMUECR application version numbering methodology what is based on common Verifone Baltic version numbering policy for terminal payment applications (reference *(4) Verifone Baltic – Terminal Software Version Numbering Specification v1.4.1*)

Application version numbering format:

<NNNNNNNNNN> <XX>.<YY>.<ZZZ>.<BBBBB>, where :

Format	Subject	Description
NNNNNNNNNN	Software Name;	Name of the application
XX	Major application version number	This version number indicates the major version of the payment application. It is increased every time, when major changes are done, according to PA-DSS rules. Number is never restarted within the application life cycle
YY	Payment application identifier	Number is attached to a combination of particular payment application and “major” (from PA-DSS prospective) payment functionality. For current application it has fixed value: 21 – Merchant Unit Application, main configuration;
ZZZ	Minor application version number	This number is increased every time some changes to the functionality of the application are done, which are not considered “major” by PA-DSS rules for payment application. Number can be (but not mandatory should be) restarted, when “Payment application major version number” or “Payment application identifier” is changed. In cases, when changes contain only bug fixes of existing functionality, but functionality itself isn’t changed, minor application number should not be increased
BBBBB	build number	Increased every time, when new software package is created, even on minor bug fixes, when no changes to neither version numbers are made. Number is never restarted during the application life cycle. Should mandatory present, but should not be mandatory presented to external parties, when indicating application version. If a new package contains changes what could be classified as Low-impact or High-impact from PA-DSS prospective than together with build number other relevant part of version number MUST be changed

Example: let's look on PBMUECR 04.21.004.00160:

PBMUECR	Software Name;
04	Major application version number
21	Merchant Unit Application
004	Minor application version number
00160	build number

A3 Instances where PAN is displayed

Below represented instances where PBMUECR application can show cardholders data:

Instance	Description	Protection
DISPLAY	Manual PAN entry dialog	none
ECR protocol: Account Data to PED	Regular transaction. PBMUECR sends Account Data to PED application over RS232 cable for transaction processing	Encrypted according to ECR integration protocol

A4 Application components and used protocols

PED application supported by PBMUECR terminals:

Merchant Unit PBMUECR version	PED application MultiPOINT version
04.21.004.xxxxx	05.20.074.xxxxx 06.20.075.xxxxx

Terminal to ECR protocol in use:

List of supported protocols available in application release notes.