Verifone

Pci Pa Dss

PBMUECR 03.21.003.xxxxx Implementation Guide

Author: Sergejs Melnikovs

Filename: D01_PBMUECR_Implementation_Guide_v2.1.docx
Version: 2.1
Date: 2015-11-23

Contents

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 running on your PBMUECR on that list please contact our helpdesk at Verifone 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 PBMUECR application. Verifone 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 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.

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

1.4 Update History

Ver.	Name	Date	Comments
1.0	Sergejs Melnikovs	2013-05-23	First release
1.1	Sergejs Melnikovs	2013-07-09	Added application version on title page
1.2	Sergejs Melnikovs	2013-07-17	Added notes in chapter 3 and sowtware dependences in chapter 2.3.1
1.3	Sergejs Melnikovs	2014-07-17	Annual review, minor changes according to PBMUECR version 02.21.002 functionality. Added description of version numbering methodology
2.0	Sergejs Melnikovs	2015-06-25	Document rebranding. Updated according to PCI DSS & PCI PA DSS version 3.1 requirements
2.1	Sergejs Melnikovs	2015-11-23	Minor update, updated document restriction

1.5 Terminology

PBMUECR: Merchant unit application for use in Baltic States (Estonia, Latvia, Lithuania)

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.

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.

Cardholder Data: PAN, Expiration Date, Cardholder Name and Service Code.

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.

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.

SSL: Secure Sockets Layer is a commonly used method to protect transmission across public networks.

ECR: Electronic Cash Register

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. 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.

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.

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.

WEP: Wired Equivalent Privacy, a wireless network security standard. Sometimes erroneously called "Wireless Encryption Protocol".

Magnetic Stripe Data: Track data read from the magnetic stripe, magnetic-stripe image on the chip, or elsewhere.

Sensitive Authentication Data: Magnetic Stripe Data, CAV2/CVC2/CVV2/CID, PINs/PIN blocks.

POS: Point of sale

TRSM: Tamper resistant security module, sometimes used short abbreviation TRM (tamper resistant security module

3DES: Triple DES common name for the Triple Data Encryption Algorithm

AES: Advances encryption standard

TMS: Terminal management system

HSM: Hardware security module

2 SUMMARY OF PCI DSS REQUIREMENTS

This summary covers shortly the PCI-DSS/PA-DSS requirements that have a related PA-DSS Implementation Guide topic. It also explains how the requirement is handled in the PBMUECR application and also explains the requirement from your aspect.

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 Protecting sensitive cardholder data

2.1.1 Requirement 1: Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2), or PIN block data

a. What the requirement says

Do not store sensitive authentication data after authorization. Only those data elements needed for business should be stored.

b. How the PBMUECR application meets this requirement

No specific setup for the PBMUECR application is required. PBMUECR application never stores Sensitive Authentication Data (Full Magnetic Stripe, CVV/CVV2, PIN/PIN Block).

c. What this means to you

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.

2.1.2 Requirement 1.1.4: Historical data deletion

a. What the requirement says

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
Aligns with PCI DSS Requirement 3.2

b. How the PBMUECR application meets this requirement

No specific setup for the 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.

c. What this means to you

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.

2.1.3 Requirement 1.1.5: Securely delete any sensitive data used for debugging or troubleshooting

a. What the requirement says

Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files.

Aligns with PCI DSS Requirement 3.2

b. How the PBMUECR application meets this requirement

No any sensitive cardholder's data are retrieving by PBMUECR application in 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.

c. What this means to you

No actions needed.

2.1.4 Requirement 2: 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 network 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 PAN in unencrypted e-mails.

b. How the PBMUECR application meets this requirement

PBMUECR application never stores Sensitive Authentication Data (Full Magnetic Stripe, CVV/CVV2, PIN/PIN Block). For transactions Cardholder Data (PAN, Expiry Date, Cardholder Name and Service Code) are sending to PED over RS232 cable encrypted by public part of RSA of connected PED. During startup process PED provides public key to PBMUECR application and then PBMUECR doesn't store it on any local storage.

Regarding PAN masking, however, there may be some banks requirement of printing full PAN on merchant receipt for offline transactions. PBMUECR application share the printer to PED application and is not responsible for content of the receipt. PBMUECR doesn't store any information of the receipt after printing is done.

c. What this means to you

For cards read by the PBMUECR application magnetic stripe 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 the PAN, expiration date or CVV2. In case you have any suspicions that the terminal could have been tampered with you have to stop making transactions and immediately contact service provider.

2.1.5 Requirement 2.1: Purging cardholder data

a. What the requirement says

Software vendor must provide guidance to customers regarding purging of cardholder data after expiration of customer-defined retention period.
Aligns with PCI DSS Requirement 3.1

b. How the 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.

c. What this means to you

No action needed.

2.1.6 Requirement 2.2: Mask PAN when displayed

a. What the requirement says

Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.
Aligns with PCI DSS Requirement 3.3

b. How the PBMUECR application meets this requirement

Details of all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts are available in Annex *A3 Instances where PAN is displayed*

c. What this means to you

If the terminal prints full PAN on merchant ticket 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.

2.1.7 Requirement 2.3: Render PAN unreadable anywhere it is stored

a. What the requirement says

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)
Aligns with PCI DSS Requirement 3.4

b. How the PBMUECR application meets this requirement

Details of all instances where PAN is displayed, including but not limited to POS devices, screens, logs, and receipts are available in Annex *A3 Instances where PAN is displayed*

c. What this means to you

The customer is responsible for rendering PAN unreadable in all instances where PAN could be stored in outside of the terminal application.

2.1.8 Requirements 2.4 & 2.5: Protect keys

a. What the requirement says

Access to keys used for cardholder data encryption must be restricted to the fewest possible number of key custodians. Keys should be stored securely.

Aligns with PCI DSS Requirement 3.5 & 3.6

b. How the 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

c. What this means to you

No actions needed.

2.1.9 Requirement 2.6: Implement key management

a. What the requirement says

Key management procedures must be implemented to support periodic key change and replacement of known, expired or suspected compromised encryption keys.

Aligns with PCI DSS Requirement 3.6

b. How the 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

c. What this means to you

No actions needed.

2.2 User IDs, secure authentication and user access logging

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.

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 without system activity logs.

2.2.1 Requirement 3.1: Unique user IDs and secure authentication for administrative access

a. What the requirement says

The "out of the box" installation of the payment application in place at the completion of the installation process must facilitate use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data.

Aligns with PCI DSS Requirements 8.1 and 8.2

b. How the PBMUECR application meets this requirement

PBMUECR application does not handle administrative access control by itself – all administrative configurations handled by PED application connected to PBMUECR over RS232 cable.

c. What this means to you

No actions needed.

2.2.2 Requirement 3.2 & 3.4: Unique user IDs and secure authentication for access to servers etc.

a. What the requirement says

Access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication.
Aligns with PCI DSS Requirements 8.1 and 8.2

b. How the PBMUECR application meets this requirement

The PBMUECR application does not provide any accounts for access to PCs, servers and databases containing critical data.

c. What this means to you

No actions needed.

2.2.3 Requirement 4.1 & 4.2: Implement automated audit trails

a. What the requirement says

Payment application must implement an automated audit trail to track and monitor access.
Aligns with PCI DSS Requirement 10.1 and 10.2

b. How the PBMUECR application meets this requirement

All user access is being logged by the PBMUECR application; logging is automatically enabled “out of the box”.
The PBMUECR application does not allow making any changes relevant to the payment functionality. All relevant changes on the terminal (system level objects creation, deletion or update, configuration changes driver update, file download and etc.) could be done only through PED application connected to PBMUECR over RS232 cable.

c. What this means to you

The application uses syslog protocol for audit trails. If you need to receive this data on your syslog server too please refer *to (4) Terminal Audit Log v1.7*.

2.2.4 Requirement 4.4: Facilitate centralized logging

a. What the requirement says

Payment application must facilitate centralized logging.
Aligns with PCI DSS Requirement 10.5.3

b. How the 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 specific format and described in separate document *(4) Terminal Audit Log v1.7*

c. What this means to you

The application uses syslog protocol for audit trails. If you need to receive this data on your syslog server too please refer *to (4) Terminal Audit Log v1.7*.

2.3 Secure application development

2.3.1 Requirement 5.4: Use only necessary and secure components

a. What the requirement says

The payment application must only use or require use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality of the payment application.

b. How the PBMUECR application meets this requirement

Device with PBMUECR application should be used only together with a VeriFone hardware terminal running the dependent PA-DSS validated software MultiPOINT starting from version 03.20.072.xxxxx

c. What this means to you

No actions needed

2.4 Wireless technology and network implementation

2.4.1 Requirement 6: Protect wireless transmissions

a. What the requirement says

Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.

b. How the PBMUECR application meets this requirement

PBMUECR application doesn't support wireless communication.

c. What this means to you

If you are using wireless network within your business on your router to establish connection to a public network, 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 application 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 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

2.4.2 Requirement 6.1: Securely implement wireless technology

a. What the requirement says

For payment applications using wireless technology, the wireless technology must be implemented securely.

Aligns with PCI DSS Requirements 1.2.3 & 2.1.1

b. How the PBMUECR application meets this requirement

The PBMUECR application doesn't support wireless communication

c. What this means to you

No actions needed.

2.4.3 Requirement 6.2: Secure transmission of cardholder data over wireless networks

a. What the requirement says

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.

Aligns with PCI DSS Requirements 1.2.3, 2.1.1, & 4.1.1

b. How the PBMUECR application meets this requirement

The PBMUECR application doesn't support wireless communication.

c. What this means to you

For wireless networks transmitting cardholder data or connected to the cardholder data environment, verify that industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.

For other actions please refer to part 2.4.1c of this document.

2.4.4 Requirement 8.2: Must only use secure services, protocols, daemons and other components

a. What the requirement says

The payment application must only use or require use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality of the payment application.

Aligns with PCI DSS Requirement 2.2.3

b. How the PBMUECR application meets this requirement

Verifone terminal in “out of the box” configuration doesn’t use any unsecure protocol. The terminal accepts an application only if the application signed by valid production certificate. PBMUECR application designed to use for CHD & SAD processing only secure protocols.

c. What this means to you

No actions needed.

2.5 Data storage and remote access/updates

2.5.1 Requirement 9: Cardholder data must never be stored on a server connected to the Internet

a. What the requirement says

Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment. Limit inbound Internet traffic to IP addresses within the DMZ. Do not allow internal addresses to pass from the Internet into the DMZ.

b. How the PBMUECR application meets this requirement

PBMUECR application is designed to operate in a network behind a firewall. PBMUECR application also allows the use of DMZs.

c. What this means to you

No actions needed.

2.5.2 Requirement 9.1: Store cardholder data only on servers not connected to the Internet

a. What the requirement says

The payment application must be developed such that the database server and web server are not required to be on the same server, nor is the database server required to be in the DMZ with the web server.

Aligns with PCI DSS Requirement 1.3.7

b. How the PBMUECR application meets this requirement

PBMUECR application does not store any cardholder data in a server connected to the internet.

c. What this means to you

No actions needed.

2.5.3 Requirement 10.1: Implement two-factor authentication for remote access to payment application

a. What the requirement says

If the payment application may be accessed remotely, remote access to the payment application must be authenticated using a two-factor authentication mechanism.

Aligns with PCI DSS Requirement 8.3

b. How the PBMUECR application meets this requirement

No remote access to Verifone production terminals or the application is possible.

c. What this means to you

No actions needed.

2.5.4 Requirement 10.2.1: Securely deliver remote payment application updates

a. What the requirement says

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.

Aligns with PCI DSS Requirements 1 and 12.3.9

b. How the PBMUECR application meets this requirement

No remote access to Verifone production terminals or the application is possible.

c. What this means to you

No actions needed.

2.5.5 Requirement 10.2.3: Securely implement remote access software

a. What the requirement says

If vendors, resellers/integrators, or customers can access customer's payment applications remotely, the remote access must be implemented securely.

b. How the PBMUECR application meets this requirement

No remote access to Verifone production terminals or the application is possible.

c. What this means to you

No actions needed

2.6 Sensitive traffic/access encryption

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Miss-configured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

Use strong cryptography and security protocols such as TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.

2.6.1 Requirement 11.1: Secure transmissions of cardholder data over public networks

a. What the requirement says

If the payment application sends or facilitates sending cardholder data over public networks, the payment application must support use of strong cryptography and security protocols such as TLS and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

Aligns with PCI DSS Requirement 4.1

b. How the PBMUECR application meets this requirement

PBMUECR application does not send any cardholder data over public network. All manipulation with cardholder data handled (encrypted/stored) by PED application connected to PBMUECR over RS232 cable. PBMUECR just retransmit IP packets (received from PED) to public network.

c. What this means to you

No actions needed.

2.6.2 Requirement 11.2: Encrypt cardholder data sent over end-user messaging technologies

a. What the requirement says

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.

Aligns with PCI DSS Requirement 4.2

b. How the PBMUECR application meets this requirement

PBMUECR application is not able to send any cardholder data using end-user messaging technologies.

c. What this means to you

No actions needed.

2.6.3 Requirement 12.1 & 12.2: Encrypt all non-console administrative access

a. What the requirement says

If the payment application facilitates non-console administrative access, include instructions on how to configure the application to use strong cryptography (such as SSH, VPN, or TLS) for encryption of all non-console administrative access to payment application or servers in cardholder data environment..

Aligns with PCI DSS Requirement 2.3

b. How the PBMUECR application meets this requirement

No remote access to Verifone production terminals (nor the application) is possible.

c. What this means to you

No actions needed.

Annexes

A1 Terminal files

Below there is a table describing files that are used by PBMUECR application:

Files loaded to terminal			
File Name	Description	Can contain cardholder data	Protection
PBMUECR.OUT	Application executable file		Signed by Verifone tool
*.p7s	Signature for application/library/script file. OS will not run application/library/script that is not signed or if signature verification failed		
*.img	Image file (animation pictures, used during connection)		
*.vft	Screen font		
*.pft	Printer font		
Files that may be created during application work			
File Name	Description		Protection
#DSS.LOG	Audit log		
LOGO.LGO	Printer logo data		
TMP_LOGO.LGO	Printer logo data (temporary file)		

A2 Application Version Numbering roles

Below represented PBMUECR application version numbering methodology what is based on common Verifone Baltic version numbering policy (reference (5) *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 contains 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

So let's look on PBMUECR 03.21.003.00080:

PBMUECR	Software Name;
03	Major application version number
21	Payment application identifier
003	Minor application version number
00080	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: CHD to PED	Regular transaction. PBMUECR sends CHD & SAD to PED application for transaction processing	Encrypted according to ECR integration protocol