PA-DSS Implementation Guide for PSAM Telium II (T2/CDP) 3.1.x.x

Version 2.9

1 Introduction and Scope

1.1 Introduction

The purpose of this PA-DSS Implementation Guide is to instruct Merchants on how to implement Nets' PSAM Telium II application (aka: T2/CDP) into their environment in a PCI DSS compliant manner. It is not intended to be a complete installation guide. PSAM Telium II, if installed according to the guidelines documented here, should facilitate and support a merchant's PCI compliance.

This solution is based on PSAM/CDP and only the tiny part of the software (the CDP module) has access to card holder data. It encrypts it and sends it to the PSAM. Since the CDP module resides in the terminal no cardholder data leaves the terminal unencrypted.

For a more elaborated description of the solution please see appendix A

1.2 What is Payment Application Data Security Standard (PA-DSS)?

The Payment Application Data Security Standard (PA-DSS) is a set of security standards that were created by the PCI SSC to guide payment application vendors to implement secure payment applications.

1.3 Distribution and Updates

This PA-DSS Implementation Guide should be disseminated to all relevant application users including merchants by email. It should be updated at least annually and after changes in the software. The annual review and update should include new software changes as well as changes in the PA-DSS standard.

Updates to the PA-DSS Implementation Guide can be obtained via email by contacting Nets directly (Nets MS Sales support).

This PA-DSS Implementation Guide references both the PA-DSS and PCI DSS requirements. The following versions were referenced in this guide.

- PA-DSS version 3.2
- PCI DSS version 3.2.1

1.4 Referenced documents

Since this payment solution is based on that the PSAM executes the transactions the all transaction related topics are already covered by the PSAM Implementation guide:

[1] PA−DSS 3.2 Implementation Guide for Nets PSAM version 9.2.01.x

Any details of implementation towards PSAM is documented in the PSAM requirements specification (the OTRS):

[2] OTRS3.5.2_20180112_MS_Denmark.pdf

Referenced documents can be obtained by contacting Nets directly (Nets MS Sales support)

2 Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data

2.1 Merchant Applicability

It is the Merchants responsibility to remove any magnetic stripe data, card validation values or codes, PINs or PIN block data, cryptographic key material, or cryptograms stored by previous versions of the payment application software. However, for the PSAM Telium II application this is not necessary as none of these items are present.

To be PCI compliant, a merchant must have a data-retention policy which defines how long cardholder data will be kept. PSAM Telium II does not retain cardholder data and can be exempt from the merchant's cardholder data-retention policy.

2.2 Secure Delete Instructions

The following process is used by PSAM Telium II to automatically and securely delete prohibited historical data and to purge cardholder data after expiration:

Any instance of prohibited historical data that exists in a terminal will be automatically deleted securely when PSAM Telium II payment application is installed on the terminal. Deletion of prohibited historical data and data that is past retention policy will happen automatically.

2.3 Locations of Stored Cardholder Data

The CDP Component never store cardholder data.

Customers are requested to perform an advice transfer, before switching PSAM. The payment solution automatically perform advice transfer before PSAM updates are performed.

2.4 Troubleshooting Procedures

When troubleshooting issues, care must be taken to properly protect cardholder data:

- Collect sensitive authentication data only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete such data immediately after use.

Nets support will not request sensitive authentication or cardholder data for troubleshooting purposes.

Telium II terminal can be from factory be set up as production mode or as “Mockup” (debug mode). In “Mockup” mode the terminal can only be key loaded with test keys, and operate using test PSAM’s, and communicating with the test host. Alternatively a terminal produced to be production can only be keyloaded with production keys in the secure key load facility, have to use production PSAM and communicate with the production hosts.

PSAM Telium II do not support collecting or logging of cardholder data for terminals in production mode. In debug mode (aka Mockup) cardholder data is logged.

All components of the PSAM Telium II solution poses facilities for doing debug logging for technical low level debugging. This will be disabled for terminals delivered for production, but can be enabled in case an ECR integrator encounter problems which need to be debugged. This process is handled by Nets MS Sales support. Since debug logging slows down the terminals, disable it after use. In production mode the debug log holds status information, low level trace information, but no card holder data. Card holder data can be logged in “mockup” terminals when running a special logging enabled application.

The PCI PA DSS is only applicable for terminals in production mode.

2.5 Key management

For the Telium 2 range of terminal models, all security functionality is performed in a secure area protected even from the payment application.

Encryption of cardholder data are performed by the CDP module and decrypted by the PSAM. The PSAM then re-encrypt with the proper keys for the host communication.

Procedures for Key Management are implemented by Nets according to the PSAM requirement specification.

The key management is independent of the payment functionality. Loading a new application therefore does not require a change to the key functionality.

2.6 PAN displayed/printed locations

Masked PAN:

- Financial Transaction receipts:
  Masked PAN is always printed on the transaction receipt for both cardholder and merchant. The masked PAN in most of the cases is last 4 digits.
- Transaction list report:
  Transaction list report shows the transactions performed in a session. Transaction details includes Masked PAN, Card issuer name and the transaction amount.
- Last customer receipt copy:
  The copy of last customer receipt can be generated from terminal menu. The customer receipt contains the masked PAN as the original customer receipt. The given function is used in case if terminal fails to generate a customer receipt during the transaction for any reason.

Confirmation:

T2/CDP always encrypts the cardholder data by default for all transactions and sends encrypted card data towards PSAM.

To display or to print the card PAN, T2/CDP always masks the PAN digits with asterisk ‘*’ except the Last 4 digits which are in clear by default.

3 Password and Account Settings

3.1 Access Control

The PSAM Telium II payment application does not have user accounts giving access to card holder data, so there are no corresponding passwords.

3.2 Password Controls

The PSAM Telium II payment application does not have user accounts or corresponding passwords, giving access to cardholder data; therefore the PSAM Telium II application is exempt from this requirement. However, some interface components do have passwords for restricting merchant access to certain settings of the interface components and for statistical purposes. These are out of scope for this description as stated above.

For the merchants general knowledge listed below are the PCI password requirements.

- Customers are advised against using administrative accounts for application logins (e.g., don't use the "sa" account for application access to the database).
- Customers are advised to assign strong passwords to these default accounts (even if they won't be used), and then disable or do not use the accounts. Customers are advised to assign strong application and system passwords whenever possible.
- Customers are advised how to create PCI DSS-compliant complex passwords to access the payment application. Customers are advised to control access, via unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

Passwords should meet the requirements as shown below:

- Do not use group, shared, or generic accounts and passwords.
- Change user passwords at least every 90 days.
- Require a minimum password length of at least seven characters.
- Use passwords containing both numeric and alphabetic characters.
- Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
- Limit repeated access attempts by locking out the user ID after not more than 6 attempts.
- Set the lockout duration to thirty minutes or until administrator enables the user ID.
- If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.

4 Logging

4.1 Merchant Applicability

Currently, for Nets PSAM Telium II payment application, there is no end-user, configurable PCI log settings.

4.2 Configure Log Settings

The PSAM Telium II payment application does not have user accounts, so PCI compliant logging is not applicable. Even in the most verbose transaction logging the PSAM Telium II application does not log any sensitive authentication data or cardholder data.

4.3 Central Logging

The PSAM Telium II payment solution supports central logging as required in the PSAM Requirement Document. The mechanism also includes logging of creation and deletion of SW executables.

4.3.1 Setup of Central Logging

In the PSAM/CDP concept all configuration changes are handled by Nets Cards through the PSAM. Nets Cards will have a central log showing these configurations. Nets Cards can verify that the solution is working with CDP encryption to ensure that no card data is present outside the secure modules (card reader and PSAM).

4.3.1.1 Setting up a Syslog server

If the merchant prefer to setup an "internal" central logging, it is possible to setup the Payment Middleware to direct the log towards a standard Syslog server. Syslog servers are available as open source for various platforms.

Central logging requires the Syslog server to present on the network. The log uses UDP protocol through the network.

4.3.1.2 Information provided in log

As the payment solution is started information (serial numbers, SW revisions etc.) on all components are added to the central log (start-up receipt).

All changes in the PSAM configuration are also sent to the log. This is covered in the PA-DSS evaluation of the PSAM [1]. The information provided complies with PA-DSS 3.2. Even with logging enabled, T2/CDP never logs cardholder or sensitive data in production.

4.3.1.3 Enable Merchant Central Logging on the integrated solution

This paragraph covers log setup on Nets T2/CDP solutions.

On these solutions central logging is configured in the "log4j.properties" file in the same way as the debug log. The following lines needs to be part of the file:

```
# To direct a log level "info" to the log named "central":
log4j.category.CentralLog=info, central
# To setup the routing of "central" towards the SysLog server:
log4j.appender.central= org.apache.log4j.net.SyslogAppender
# To setup ip-address and port (example)
log4j.appender.central.host=172.21.41.186
log4j.appender.central.port=9876
# To setup the format of the log
log4j.appender.central.layout=org.apache.log4j.PatternLayout
log4j.appender.central.layout.ConversionPattern=%5p %d{ABSOLUTE} - %m%n
```

4.3.1.4 Enable Logging on embedded solution

In order to enable syslog logging towards a merchant supplied syslog server:

1. press the "Menu" button.

2. Then in the menu select “Settings menu” | “Engineer menu” (press ‘8’ and ‘6’).
3. Type in the daily technician code, which you can get by phoning Nets MS support.
4. Select “Log settings” (7)
5. In the field “IP address” type in the IP address of the syslog server

Ignore any other parameter as they are for the debug log – not the central log

To disable logging towards the central server set the IP address to 0.0.0.0

4.4 Trouble shooting logging

In addition to the PCI required ‘Central logging’ this solution also facilitates trouble shooting logging. See 2.4 Troubleshooting Procedures

5 Secure Payment Application

5.1 Application SW

This payment solution consists of several SW modules. From a PCI DSS perspective the important one is the CDP module, see appendix A for a more elaborated technical description. This module executes in the secured environment inside the Telium II terminal HW. The PSAM Telium II CDP module SW executables are digitally signed, as are any module which is executing in the secured Telium II environment.

The terminal communicates with the Nets Host using TCP/IP, either via Ethernet, GPRS, Bluetooth, or the PC-LAN running the POS application.

The payment middleware always takes the initiative for establishing the communication over public WAN IP networks towards the remote hosts. For integrators using TCP locally between ECR and PSAM Telium II middleware need to implement firewall protection, shielding the merchant private network from the public Internet.

When integrated with a POS application on a PC, the terminal can be set up to communicate via the PC-LAN running the POS application using either RS232, USB or Bluetooth. Still CDP is running in the terminal and all functionality of the payment application is running in the PSAM. The installation and integration of the ECR components are handled by integrator in corporation with Nets MS Sales support. Since no component on the ECR ever process any card holder data there is no installation details of the ECR components which have PCI PA DSS implication.

The application protocol (and applied encryption) is transparent and independent of the type of communication.

1. PSAM Telium II – Payment Host communication TCP/IP parameter setup

Host IP Address	193.142.211.17
PORT	22000

2. PSAM Telium II – ECR Communication
    a. RS232 Serial
    b. USB Connection
    c. TCP/IP parameter setup, also known as ECR over IP

ECR IP Address	ECR machine's IP address
PORT	1234

5.2 Supported terminal hardwares

T2 CDP is supported on variety of PTS (PIN transaction security) validated Ingenico devices. The list of terminal hardware along with their PTS approval number is given below.

Terminal hardware	PTS version	PTS approval number
iPP350	3.x	4-20184
iWL220, iWL250	3.x	4-20181
ICT220, ICT250	3.x	4-20196

6 Wireless Networks

6.1 Merchant Applicability

PSAM Telium II does not make use of WiFi wireless technology. However, the use of wireless is possible together with PSAM Telium II, in order for Wireless to be implemented securely, consideration should be taken when installing and configuring the wireless network as detailed below.

6.2 Recommended Wireless Configurations

There are a number of considerations and steps to take when configuring wireless networks that are connected to the internal network.

At a minimum, the following settings and configurations must be in place:

- All wireless networks must be segmented using a firewall, if connections between the wireless network and the cardholder data environment is required the access must be controlled and secured by the firewall.

- Change the default SSID and disable SSID broadcast
- Change default passwords both for wireless connections and wireless access points, this includes console access as well as SNMP community strings
- Change any other security defaults provided or set by the vendor
- Ensure that wireless access points are updated to the latest firmware
- Only use WPA or WPA2 with strong keys, WEP is prohibited and must never be used
- Change WPA/WPA2 keys at installation as well as on a regular basis and whenever a person with knowledge of the keys leaves the company

7 Network Segmentation

7.1 Merchant Applicability

The PSAM Telium II CDP payment solution is not a server based payment application and resides on a terminal, with some interface components executing on the ECR. For this reason the payment application does not require any adjustment to meet this requirement.

For the merchant's general knowledge, credit card data cannot be stored on systems directly connected to the Internet. For example, web servers and database servers should not be installed on the same server. A DMZ must be set up to segment the network so that only machines on the DMZ are Internet accessible.

8 Secure Remote Software Updates

8.1 Merchant Applicability

Nets securely deliver remote T2/CDP payment applications updates. These updates occur on the same communication channel as the secure payment transactions, and the merchant is not required to make any changes to this communication path for compliance.

For general information, merchants should develop an acceptable use policy for critical employee-facing technologies, per the guidelines below for VPN, or other high-speed connections, updates are received through a firewall or personal firewall.

- Use a firewall if the computer is connected via VPN or other high-speed connection, and to secure these connections by limiting only the sockets necessary for the application to function.
- Only activate remote access when needed and immediately inactivate after use.
- Nets contact cashier and/or customer and agree to an update schedule with email, when release notes and payment applications updates available. Customers can also view the latest updates, instructions, and the Implement Guide here.

8.2 Acceptable Use Policy

The merchant should develop usage policies for critical employee-facing technologies, like modems and wireless devices. These usage policies should include:

- Explicit management approval for use.
- Authentication for use.
- A list of all devices and personnel with access.
- Labelling the devices with owner.
- Contact information and purpose.
- Acceptable uses of the technology.
- Acceptable network locations for the technologies.
- A list of company approved products.
- Allowing use of modems for vendors only when needed and deactivation after use.
- Prohibition of storage of cardholder data onto local media when remotely connected.

8.3 Personal Firewall

Any "always-on" connections from a computer to a VPN or other high-speed connection should be secured by using a personal firewall product. The firewall is configured by the organization to meet specific standards and not alterable by the employee.

8.4 Remote Update Procedures

Update of transaction configuration parameters (which are stored in PSAM) is done automatically in combination with a batch data transfer. Update of PSAM application itself is done in the same way. Update of the terminal software is done via a menu entry (a manual trigger), by a timer or controlled from the ECR.

9 Remote Access

9.1 Merchant Applicability

PSAM Telium II cannot be accessed remotely. Remote support only occurs between a Nets support staff member and the merchant over the phone or by Nets directly onsite with the merchant.

9.2 Remote Access Software Security Configuration

If remote access is implemented into the environment, the following secure configurations must be considered:

- In addition to username and password and multi factor must be implemented, such as, but not limited to:
  - Personal certificates
  - OTP token
  - Smart card
- Use only secure protocols for remote access such as TLS, SSH, IPSEC or encrypted VPN
- Do not use default passwords for remote access
- Configure the firewall to only allow trusted sources for remote connections
- Implement and enforce strong access controls and passwords according to industry accepted standards, at a minimum according to PCI DSS requirement 8.x.

- Do not allow 3rd party access by vendors and resellers unless absolutely necessary and only allow such connections under a limited period of time.

10 Transmission of Cardholder Data

10.1 Transmission of Cardholder Data

PSAM Telium II utilizes the PSAM for doing transaction. Any data send over public networks to the processor (Nets) is encrypted by the PSAM. See the PSAM PA-DSS implementation guide [1] for details.

10.2 Email and Cardholder Data

PSAM Telium II does not support the sending of email. Cardholder data should never be sent unencrypted via email.

10.3 Non-Console Administrative Access

PSAM Telium II does not support Non-Console administrative access. However, for the merchants general knowledge, Non-Console administrative access must use either SSH, VPN, or TLS for encryption of all non-console administrative access to servers in cardholder data environment. Telnet or other non-encrypted access methods must not be used.

11 PSAM Telium II CDP Versioning Methodology

11.1 Versioning of the in terminal interface component

The in terminal components are version numbered according to the Ingenico versioning philosophy. A four digits number 'abcd'. For readability it is often shown as a.b.c.d where:

An increment of	Indicates
a:	Major updates. This is a significant functional update. It may include changes with impact on security or PA-DSS requirements.
b:	Minor upgrades. This is a non-significant functional update. It may include changes with impact on security or PA-DSS requirements.
c and d:	Indicate a bug fixing in a patch release. This is a non-significant functional update. It may not include changes with impact on security or PA-DSS requirements.

12 PA-DSS Requirements Reference

Chapter in this document	PA-DSS Requirements Reference
Chapter 2 : Secure Deletion of Sensitive Data and Protection of Stored Cardholder Data	1.1.4 1.1.5 2.1 2.4 2.5 2.6
Chapter 3 : Password and Account Settings	3.1 3.2
Chapter 4 : Logging	4.1 4.4
Chapter 5 : Secure Payment Application	8.2
Chapter 0 : Wireless Networks	6.1 6.2 6.3
Chapter 7 : Network Segmentation	9.1
Chapter 8 : Secure Remote Software Updates	10.2.1 10.2.3
Chapter 9 : Remote Access	10.1
Chapter 12 : Transmission of Cardholder Data	11.1 11.2 12.1 12.2
Chapter 11 : PSAM Telium II CDP Versioning Methodology	5.4.4

13 Glossary of Terms

TERM	DEFINITION
Cardholder data	Full magnetic stripe or the PAN plus any of the following: • Cardholder name • Expiration date • Service Code
CDP	Cardholder Data Protection. The way sensitive cardholder data is encrypted and transported in and out of the PSAM

ECR	Electronic Cash Register. The merchant cash register which are integrated with the payment solution.
Merchant	The end user and purchaser of the PSAM Telium II product.
PA-DSS	Payment Application Data Security Standard. PA-DSS is the Council-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP)
PA-QSA	Payment Application Qualified Security Assessors. QSA company that provides services to payment application vendors in order to validate vendors' payment applications.
PSAM	Purchase Secure Application Module. A SIM style CPU which perform the payment transactions and encrypt the host data (offline and online)
PSAM/CDP	See PSAM and CDP
Sensitive Authentication Data	Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction. Sensitive Authentication Data must never be stored when a transaction is finished.
PSAM Telium II (T2/CDP)	The software platform used by Nets for application development for the European market when a PSAM is involved in the solution and when the CDP encryption is implemented in Ingenico Telium II terminals.

14 Document Control

Document Information

Document Reference:	PSAM Telium II Implementation Guide Telium
Document Location:	Undisclosed

Summary of Changes

Version Number	Version Date	Nature of Change	Change Author	Date Approved
2.9	05.07.2019	Updated based on input from QSA	Shamsher Singh	
2.8	26.06.2019	Updated based on input from QSA	Shamsher Singh	
2.7	07.02.2019	Updated based on input from QSA	Shamsher Singh	
2.6	19.09.2018	Updated version and section 1.4	Kevin Rodrigues	
2.5	09.11.2017	Updated section 4.3.1.2, 4.3.1.3 and updated reference to PADSS v3.2	Shamsher Singh	
2.4	1.09.2017	Updated reference to new PSAM Implementation guide & section 11.1.	Shamsher Singh	
2.3	17.08.2017	Updated Document Approvals	Seija Salo	
2.2	7.12.2015	Updated based on input from QSA	Lars Worsaae	
2.1	26.10.2015	Updated based on review input	Lars Worsaae	
2.0	20.10.2015	New document based on One PA	Lars Worsaae	

	implementation guide

Distribution List

Name	Function
Terminal Department	Development, Test, Project Management, Compliance
Product Management	Terminal Product Management Team, Compliance Manager – Product

Document Approvals

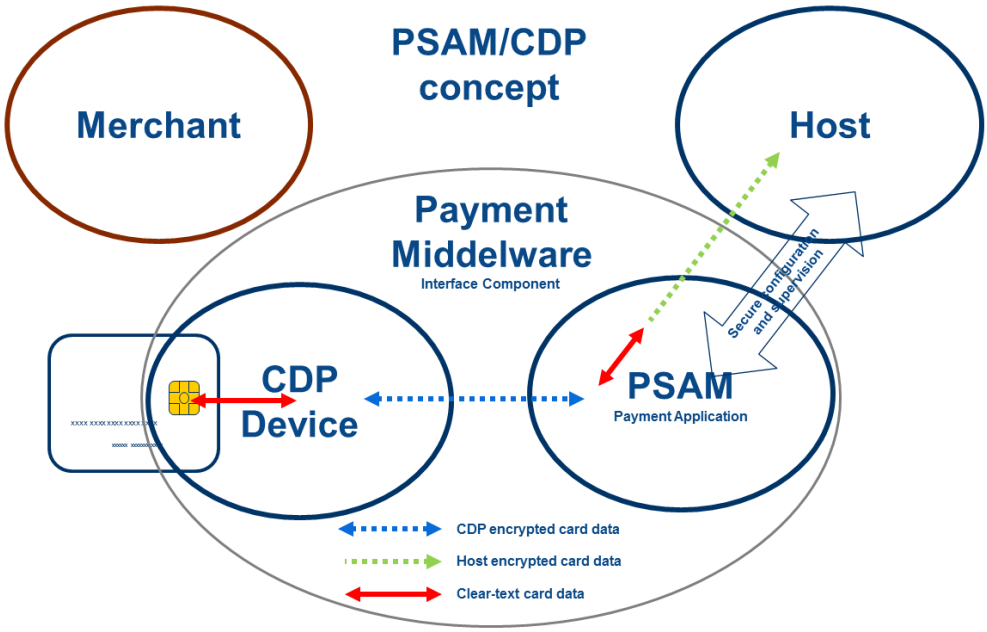
Name	Function
Mikko Jokelainen	Engineering Manager

Appendix A: Description of the Payment Solution

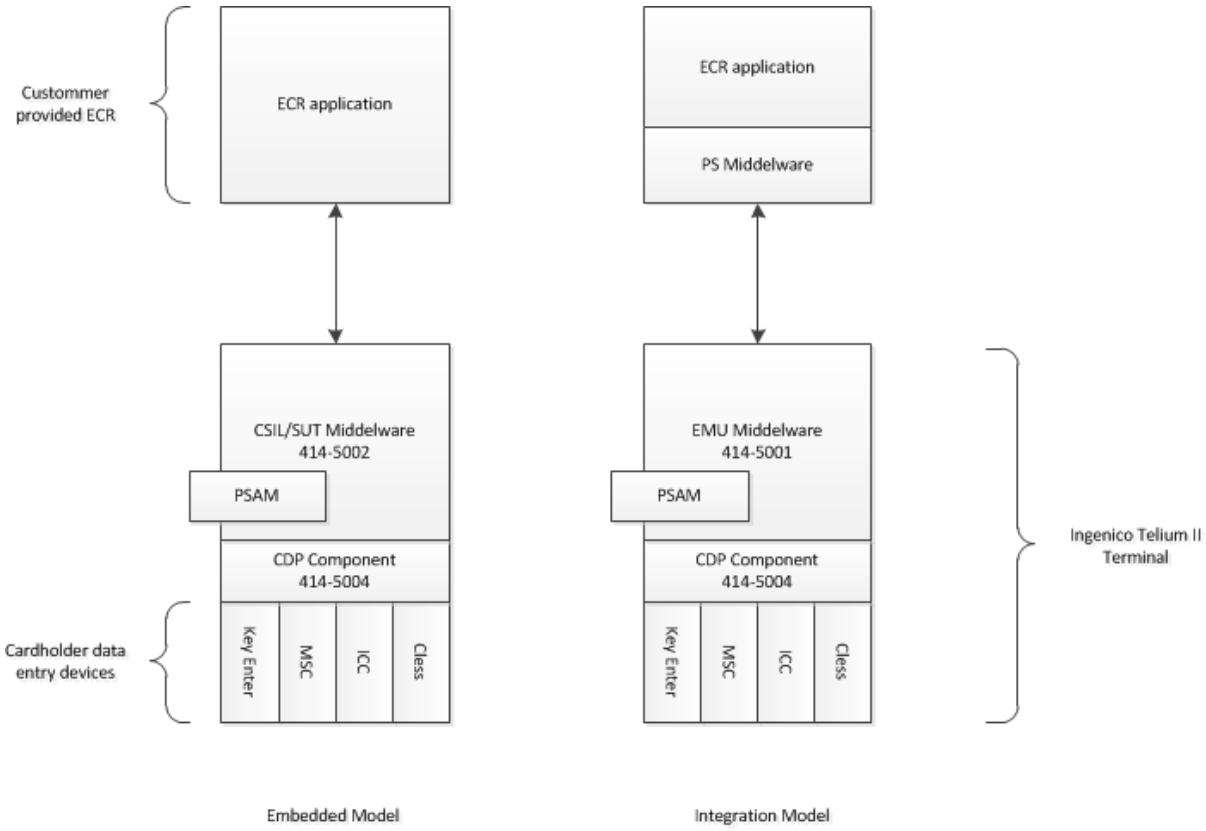
The central component of any PSAM based payment solution is the PSAM. Inside the PSAM executes the payment application protected by the secure environment of the PSAM.

The other component of importance in a PSAM / CDP solution is the CDP component. The responsibility of this is to encrypt cardholder data from the card readers before it is send to the PSAM. In the PSAM Telium II solution the CDP component is installed within the application zone of the Telium II terminal. This component interacts directly with the chip card reader, magnetic stripe reader and PIN Pad. All cardholder data transmitted by the processing component is encrypted using keys provided by the PSAM, thereby ensuring that it is only the PSAM which can decrypt the cardholder data.

In order for the PSAM to access physical hardware and external services as ECR, printer, TCP/IP resources, disk storage and communicate with the CDP component the payment middleware exist.



Depending upon the configuration, the interface component is either installed in the application zone of the PED (Embedded Model), or on the Point of Sale (Integration Model). Irrespective of the configuration (Integration or Embedded), the interface component only handles encrypted cardholder data and never handles cardholder data in the clear. In the Embedded Model, the interface component is a C application, in the Full Integration Model it is a Java application. The processing component is a C application in both models.



The CDP component of PSAM Telium II receives cardholder data read from the card (including track 2 from the magnetic stripe, track 2 equivalent data from the chip or contactless and the key entered data for a key entered transaction). The CDP component encrypts the cardholder data according to the PSAM specification (See PSAM implementation guide) and passes it to the middleware component. The middleware component in turn passes the encrypted cardholder data to the PSAM application. The encryption key used by the CDP component is shared with the PSAM application which enables the PSAM to decrypt the cardholder data to generate the authorisation request for subsequent transmission to the processor (Nets). A new encryption key is derived at every session (card insertion).