

Security Requirements for an EFTPOS Terminal

Version: 1.2.1

CONTENTS:

VERSION HISTORY	3
1 SCOPE.....	3
2 SYSTEM OVERVIEW	3
2.1 ONLINE DEBIT/CREDIT TRANSACTION PROCESSING.....	3
2.2 OFFLINE DEBIT/CREDIT TRANSACTION PROCESSING	4
2.3 MULTI-APPLICATION ASPECTS	4
3 GENERAL SECURITY REQUIREMENTS	4
3.1 THE SA ROLE.....	5
3.2 PIN PROTECTION	5
3.3 SDA AND DDA KEY PROTECTION	6
3.4 MESSAGE AUTHENTICATION.....	6
3.5 DATA ENCRYPTION.....	6
3.6 SOFTWARE MANAGEMENT AND PROTECTION.....	6
3.7 PARAMETER PROTECTION	7
4 TERMINAL SECURITY.....	7
4.1 THE TERMINAL CONTAINS A SECURE DEVICE	7
4.2 THE TERMINAL CONTAINS A PROTECTED AREA	7
4.3 THE TERMINAL IS AN ONLINE-ONLY TERMINAL	7
4.4 THE TERMINAL IS ONLY POSSIBLE TO LOAD IN A SECURE ENVIRONMENT.....	7
5 OPEN APPLICATION IMPLEMENTATION	8
5.1 LOAD CLIENT.....	8
5.2 REVIEW AND FREEZING	8
6 PIN MANAGEMENT APPLICATION IMPLEMENTATION	8
6.1 REVIEW AND FREEZING	8
6.2 SOFTWARE CONTROL.....	8
7 TRANSACTION DATA AUTHENTICATION AND PROTECTION.....	9
7.1 SCOPE.....	9
7.2 DATA FIELDS TO PROTECT	9
7.3 ACCESS CONTROL MANAGEMENT	9
7.4 MESSAGE AUTHENTICATION.....	10
7.5 DATA ENCRYPTION.....	10
8 KEY MANAGEMENT	10
8.1 INITIAL KEY LOADING (PERSONALISATION).....	10
8.2 KEY PREPARATION	10
8.3 KEY SEPARATION	10
8.4 KEY STORAGE.....	11
8.5 KEY DISTRIBUTION	11
9 HARDWARE ASPECTS ON A PED	11
9.1 COLOUR CODING OF KEYS	11
9.2 SPECIAL FUNCTION KEYS.....	11
9.3 PROTECTIVE SHIELD	11
REFERENCES	12
GLOSSARY	12

Version history

Date	Version	Description	Issued/revised by
2003-01-20	1.0.0	Approved by SÄKO-I.	SÄKO-I
2004-06-30	1.1.0	The SA role more expressed. Load client certification is the responsibility of the SA and text is thus moved to guideline. Removed reference to CASH.	SÄKO-I
2006-03-03	1.2.0	Requirements for data protection incorporated. More consistent description of SA. References to PCI. References to SAC.	Hans Olof Andersson
2006-03-16	1.2.1	Editorial adjustments. Approved by PNC SAC.	PNC SAC

1 Scope

This document specifies the security required for terminals and other card accepting devices that are going to be used in systems, which shall fulfil requirements defined by the Pan Nordic Card Association, PNC. These mandatory security requirements shall be valid for all POS terminals used for acquiring in Sweden.

The PNC Security Advisory Committee, SAC, is responsible for the documentation of the requirements. PNC SAC is the security committee jointly appointed by PNC member banks. The PNC SAC is thus acting on behalf of all PNC card issuing and acquiring banks.

The fulfilment of the requirements presented in this document shall be subject to approval by the acquirer.

As a complement to the requirements from this document, PNC SAC has issued a set of guideline documents covering various aspects on PIN and PED management, but also for software and parameter management. These guidelines are meant to serve as a help for parties designing PED and implementing a PIN managing application. One purpose is also to achieve a uniformed function for card and PIN handling.

The basis for all PNC SAC documents are the PCI requirements for PIN security as defined by ref[pcipin], PED as defined by ref[pciped] and for data security, DSS, as defined by ref[pcidss].

2 System overview

2.1 Online debit/credit transaction processing

For the system overview we define 5 levels of transaction processing, the card, the terminal, one or more processing centre(s), the acquirer and the issuer. For an EMV transaction we then will have the cryptographic zones shown in fig. 1.

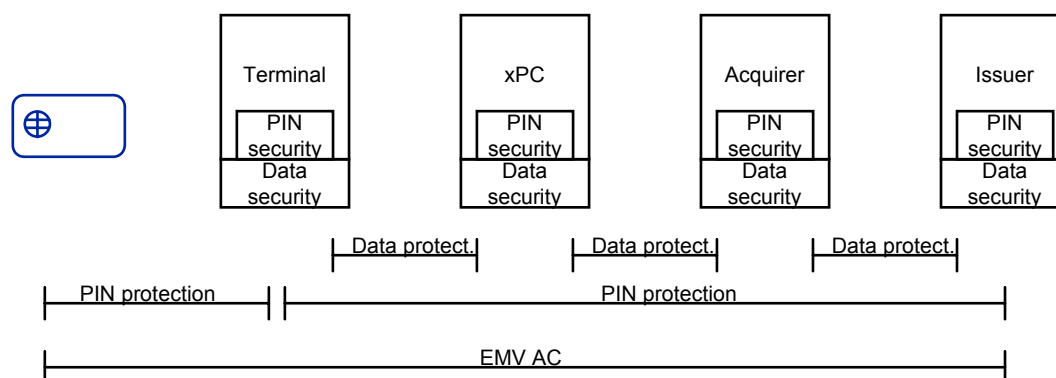


Fig. 1.

The Application Cryptogram, AC, defined by EMV forms a cryptographic zone from the card to the card issuer system. The requirements for this zone are not a part of this document.

There has to be a strong protection for the PIN from terminal to issuer (in the case of online PIN) or from terminal to chip (in the case of offline PIN). Re-encryption of PIN, always under the responsibility of one acquirer, will have to take place when changing from one zone to another. Such re-encryption will have to take place within a secure device. More about this may be found in ref[sacson].

Data protection is normally between nodes. Decryptions or MAC verifications are normally performed before any processing takes place within a node. A new encryption or MAC calculation is normally performed before passing a transaction on to the next node. A terminal which communicates with more than one node needs to have different encryption keys for each node.

For software and parameters it is assumed that they will be distributed online and that cryptography then has to be used to protect the integrity and secrecy of the distribution process.

2.2 Offline debit/credit transaction processing

As one purpose with EMV is to make it possible to increase the ratio of offline processing, this leads to higher requirements on the authenticity of the software and parameters for the terminal. In this case the acquirer are facing a risk if a terminal neglects the mandatory checks or is using the wrong authentication parameters, like floor limits, public CA keys, etc.

2.3 Multi-application aspects

A terminal that supports multi-application has by necessity to be highly reloadable. Thus an EMV terminal shall have a secure function for accepting and loading software and parameters that authenticates these before allowing them to become active in the terminal. Such a function has been named PPL (Program and Parameter Load) client, see also sections 3.6 and 5.1. The PPL client shall use a secure device or similar techniques for the cryptographic authentication of the loaded item. Fig. 2 shows an overview.

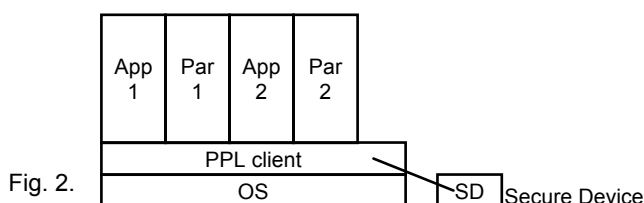


Fig. 2.

3 General security requirements

The security of handling card payments and especially the handling of PIN and PED is guaranteed by

the acquiring bank. There is a set of rules that has to be applied to situations where cards and PINs are going to be used. It is the responsibility of the acquiring bank to verify and certify that these rules are followed. These requirements are today issued under the common name PCI, Payment Card Industry and covers PIN security, ref[pcipin], PED security, ref[pciped], and data security (DSS), ref[pcidss].

This section is covering the requirements for the following:

- SA role
- PIN protection
- SDA and DDA key protection
- message authentication
- data encryption
- SW management and protection
- parameter protection.

Separate sections are also covering the requirements for

- terminal security
- open application implementation
- PIN management application implementation
- transaction data authentication and protection
- key management
- HW aspects on a PED

3.1 The SA role

The acquiring bank for this task will appoint a security administrator, SA, which externally will represent the acquiring bank in security matters.

The number one task for the SA is to assure that the security requirements for the terminal are fulfilled. In doing so the SA will be responsible for achieving the necessary security approvals. The SA shall always be able to communicate the applicable security requirements to the parties involved.

An SA may be appointed jointly by more than one acquirer. In some cases the acquirer has delegated the task to appoint SA to a processing centre. Such a delegation may be for smaller or larger parts of the security areas. Regardless of the delegation, it is always the acquiring bank that is responsible for the merchants' and processing centres' fulfilment of the requirements of the card brands.

3.2 PIN protection

The protection of PIN from intentional or unintentional exposure is the main goal for all aspects on how to implement PIN and key management. The basis for such security requirements are mainly the ISO standard, ref[iso95641], and the EMV standard, ref[emvbook2]. The international card schemes are then emphasising this in various ways. The PCI PIN security requirements, ref[pcipin], are only one example of this.

A high level summary of the requirements is:

1. PIN shall be encrypted using a method with an accepted security level.
2. When transferred from a PED to an IFD, the PIN shall have the same level of physical or logical protection as when transmitted online to issuer.
3. Cryptographic keys shall be stored and used in such a way that there is no possibility to expose the value of the key directly or indirectly.
4. Cryptographic keys shall be stored and used in such a way that there is no possibility to use the key for another purpose than the intended one.
5. Cryptographic keys loaded in clear shall be possible to load as separate components that are combined within the secure area of the PED.
6. Before loading cryptographic keys (in clear) it shall be possible to authenticate the security software in the PED.
7. Cryptographic keys shall be possible to dedicate for a certain PED.
8. All cryptographic keys, also those used for the loading of other keys, shall be possible to replace,

- e.g. when changing SA for one or more PEDs.
9. All numeric keyboard entry shall be echoed to the display. Echoing with replacement characters is only allowed for PIN entry. For all other numeric entry, the pressed digits must appear on the display.
 10. The fulfilment of security requirements shall be supervised by a SA (representing the acquiring bank).

A PIN Entry Device shall fulfil the requirements as defined by ref[pciped].

The encryption of PIN is mainly covered by ref[emvbook2] and ref[iso95641]. A more detailed implementation guideline may also be found in ref[sacalgo].

When PIN is online to issuer the terminal shall use UKPT, ref[sacalgo], the de facto standard method for PIN encryption. Should another method be suggested it has to be presented to PNC SAC for approval.

PIN offline shall comply with the requirements of ref[emvbook2]. Both clear and encrypted PIN shall be supported. If the APDU information for an ICC has to be included in the protected PIN command this encryption will have to be done in the PIN management software of the PED.

Please note that when security requirements are fulfilled by means of a secure cryptographic zone between the PED and the IFD, this zone is to be regarded as a bank zone controlled by the SA. In some cases such an implementation may require that all commands to an IFD are processed via the PED.

A PED may be used to process other PIN methods, e.g. functions for PIN to a merchant proprietary card. In such a case the approval of the SA is required.

3.3 SDA and DDA key protection

The integrity of the keys involved in the card authentication for EMV, CAM, have to be granted by the terminal as described in section 4.

Ref[emvbook2], section 11.2, shall apply to the management of SDA or DDA keys done by a terminal.

3.4 Message authentication

All card related messages between a terminal and its associated processing centre shall be protected against unauthorised modifications. Different cryptographic keys must be used for each processing centre to which the terminal has a communication link. The method used may depend on the message processing system.

For transactions with PIN it is recommended to use the MAC method defined by UKPT. For transactions without PIN, and where UKPT is not used, it is recommended to use MAC according to ISO. More about the recommended MAC methods is found in ref[sacalgo].

3.5 Data encryption

Card data shall be encrypted whenever transported in open networks. The method used may depend on the message processing system. Data encryption, when required, shall comply with the methods defined by ref[sacalgo]. A terminal shall support at least one data encryption method.

3.6 Software management and protection

The operation of secure program and parameter loading is by definition guaranteed by the organisation having the role as a Terminal Service Provider, TSP. This role must be responsible to ensure that necessary tests have been made, and in addition that only the approved software is loaded into the terminal. It is even possible that both the SA and the TSP roles are performed by the same organisation.

The organisation having the role of TSP must be clearly stated and known by all parties having a relation with the merchant in question.

All applications that are distributed through an open channel shall be independently authenticated before allowing it to become operable. Such authentication shall be based on digital signatures or a similar technique. A guideline for this may be found in ref[sacppl].

PIN managing software must reside in a protected area and shall be signed using a separate key.

The functions used to verify these signatures, before any distributed software can be accepted and stored, must be loaded into the terminal in a secure environment approved by the SA.

In the software development and distribution processes, there shall be a version management system, making it possible to have an audit trail. Such an audit trail shall show all steps taken during the life-time of a software component.

3.7 Parameter protection

Parameters distributed online to a terminal shall require message protection and/or data encryption. Parameter files shall be independently authenticated before becoming operable. Such authentication shall be based on digital signatures or a similar technique. The functions used to verify these signatures must initially be loaded into the terminal in a secure environment approved by the SA. A guideline for this protection may be found in ref[sacppl].

4 Terminal security

With EMV the offline card authentication is based on a public key hierarchy, where the root public keys are stored in the terminal. Since the protection of such keys will be critical for the future protection against false and copied cards, it is important to define security for such keys. The requirements for protection of software and parameters (especially CAM keys and PPL keys) are considered to be met in the 4 cases listed in this section.

4.1 The terminal contains a secure device

The terminal contains a secure device, e.g. in the form of a Secure Application Module, SAM, or a PIN Entry Device, PED. Such a secure device shall then be approved by PNC SAC.

4.2 The terminal contains a protected area

The terminal contains a protected area where cryptographic keys may be stored and cryptographic functions executed. Such a secure area shall be under the control of the SA. Software that may read or write in this protected area shall be signed by the SA, and the signature checked before loading the software into the terminal. The integrity of the keys shall be verified for every event that might influence the keys.

4.3 The terminal is an Online-Only terminal

The terminal is an Online-Only terminal. All transactions shall be authorised by the issuer. Card authenticity, CAM, is based on the issuers' verification of the Application Cryptogram, AC, or CVV/CVC. The PIN verification is also done by the issuer.

4.4 The terminal is only possible to load in a secure environment

The terminal may only be loaded with software and parameters (including keys) in an environment controlled by the SA. Thus the terminal will have to be loaded prior to delivery and installation.

5 Open application implementation

The open part of the terminal application shall be managed using a change and version management system. The methods used shall give a trace that makes it possible to audit every change in the software. It shall also in some aspects be possible for the acquirers' representative to certify the application, should the security and quality requirements demand such a certification.

The liability boundary, where the specifications and other information are delivered from the SA to the merchant (terminal), must be clearly defined. The dynamic nature of current and future card payment systems implies that application software and processing parameters will change rather frequently. To be able to manage this practically it is assumed that software and parameter distribution will be done electronically and protected with cryptographic methods, like digital signatures. This also makes it important to manage the cryptographic keys needed with a good security level.

5.1 Load client

One important purpose of the EMV standard is to provide possibilities of increased offline transaction processing. This means that the terminal itself will take additional decisions regarding the progress and result of the authorisation of a transaction.

Important issues are in this case the authenticity and the correctness of terminal software and any processing parameters, including such as the public keys of the CA in question. The part of the terminal software that performs such authentication of loaded software and parameters is called a load (PPL) client.

Recommendations for the implementation of a PPL client are given in ref[sacppl].

5.2 Review and freezing

The acquirer or the processing centre on behalf of the acquirer is normally responsible for the correct behaviour of a terminal application. This is often granted via a certification process that shall end in a freezing of the software. The freezing shall be closely connected to a possible signing process for the software. The remote loading of software into a terminal shall be possible only after it has been signed.

6 PIN management application implementation

The PIN management application of a terminal shall be physically or logically separated from other (open) applications parts of the terminal. It is recommended that such an implementation follows the samples set by ref[sacpedrec].

6.1 Review and freezing

Before taking a terminal into operations, its PIN management software shall be reviewed. The main purpose of this review is to detect accidental or deliberate security flaws and freeze a reference copy of the software for a possible later audit. The freezing shall be closely connected to a possible signing process for the software. The purpose of the signing is to serve as a mean to authenticate the software loading.

6.2 Software control

The loading of PIN management software in a terminal shall be possible only after the reviewed software has been signed.

It shall not be possible for a vendor to issue a new PIN management software version and take it into

operation without the SA's approval.

7 Transaction data authentication and protection

There is a rising need to prevent that cardholder account data may be used to make copies of magnetic stripe cards or as a base for making fraudulent transactions simulating "card not present" situations. The problem has been covered by the PCI Data Security Standard, ref[pcidss].

In this section are covered the requirements for the

- access control management
- message authentication
- data encryption.

7.1 Scope

This section gives the requirements regarding how to implement data protection. There is an ongoing development of new rules for the international card schemes and this section is based on the current state of applicable documents.

Important to note is that it is a combination of physical and logical protection mechanisms that shall prevent card holder account data from being used fraudulently.

7.2 Data fields to protect

As a general rule it is important to review every need to transport and store critical data in order to minimise the exposure of sensitive data.

Transport of track 2 data and other sensitive transaction data shall be protected by encryption.

The only information contained in the track 2 of a magnetic stripe that may be stored is the following:

- PAN
- expiry date
- issue number (if relevant).

Storage of such information shall be protected by encryption or access control management.

Certain information shall never be stored, e.g. CVV/CVC values, encrypted PIN. Encrypted PINs shall not even be stored on log files.

As a consequence of the laws for protection of personal data privacy, there may also be a need to protect personal data like:

- social security number (personnummer)
- transaction amount
- time of purchase
- place of purchase
- EMV transaction counter
- etc.

7.3 Access control management

Cardholder account data shall be protected to avoid unauthorised access. This means that whenever card transaction related data is stored, it shall be stored in such a way that only persons who need to know, will have access to it.

When using a general purpose host system for data files, an access control system shall be used to identify authorised personnel and to record all accesses. Back up of account data files shall either be

encrypted or managed in a physically secure way when stored outside of the normal operations environment.

7.4 Message authentication

All transaction messages between nodes shall be protected against unauthorised modifications using cryptographic methods. Different cryptographic keys must be used for each relation between nodes. The methods used may depend on the message processing systems in question. However it is strongly recommended to use one of the recommended methods found in ref[sacalgo].

In situations where data encryption is used and the transaction data contains redundancy that may be used to authenticate the integrity of the message, it might be acceptable to use a check of the redundant data for authenticating the messages.

7.5 Data encryption

All transmissions of data over open networks shall be protected by data encryption. Since today's telecom technology may use open networks, partly or in whole, even for closed user group kind of nets, encryption is a requirement for all situations. The method used may depend on the network topography and the message processing systems in question.

If a transmission network is built with several nodes, it shall be certified that all parts of the network capabilities used are protected by encryption. If this can not be certified it is recommended to use an application level of encryption between a sending and a receiving party, end to end. In such a case it is strongly recommended to use one of the recommended methods found in ref[sacalgo].

8 Key management

The management of cryptographic keys shall comply with ref[iso11568]. For PIN management, the principles for implementing terminal key management defined in ref[sapedrec] are highly recommended.

8.1 Initial key loading (personalisation)

The manufacturer of the device shall load an initial key loading key. This key is "shared" with a key management facility (KMF). Operational keys are prepared and distributed using the initial key-loading key. In order to allow for upgrades of security software it shall be possible to reload this software without erasing the current initial key value.

8.2 Key preparation

Key preparation means preparing operational keys for distribution and use in the secure device of a terminal. A suitable KMF system shall be used for this. Key preparation is done under the supervision of the SA for the system in question.

8.3 Key separation

Any organisation that is involved in the loading of the initial key loading key must never be involved in any of the subsequent key management steps. This is especially important to observe when a terminal vendor's TMS also shall be used for key and parameter distribution!

For a multifunction terminal it is important that it is able to support key schemes with different security centres responsible for key preparation and distribution.

Keys may only be used for their intended purpose. If general key slots are used, use of control vectors,

key tagging, or similar techniques shall limit the usability of the keys.

8.4 Key storage

The level of protection of stored cryptographic keys will depend on the situation. In section 4, we define 4 cases having different security implications on a device storing cryptographic keys. PIN encryption keys may, of course, never be stored or used outside of a secure device.

In a few cases the protection of data by MAC or encryption by symmetric key cryptography, is merely a protection against an external "third party" attacking the information. In such cases it may be acceptable to store and use the keys outside a secure device, e.g. in an open terminal application.

8.5 Key distribution

Key distribution shall be possible using down line load of prepared encrypted keys. A recommended way to implement this is defined in ref[sacppl].

9 Hardware aspects on a PED

9.1 Colour coding of keys

According to international recommendations some key tops shall be colour coded. The following convention is based on ref[iso95641].

Key	Colour
ENTER	Green
CLEAR	Yellow
CANCEL	Red
Other keys	Any other colour

9.2 Special function keys

If the PED is used as a general cardholder interface it shall be possible to use special function keys. The following functions shall be supported: "PIN bypass" (EJ KOD), and "selection of debit/credit" (KONTO/KREDIT).

9.3 Protective shield

The PED shall be designed to provide privacy and confidentiality so that, during normal use, only the cardholder sees the information entered or displayed. The PED shall be installed or placed so that its immediate surroundings allow sufficient privacy to enable the cardholder to enter PIN with minimum risk of the PIN being revealed to others.

The protection for the cardholder shall meet the following requirements:

It is assumed that at least 90° of a 360° horizontal view angle is covered by the body of the card holder. Then the possibility for an observer standing by the side (anywhere within the remaining 270°) to observe the PIN entry shall be protected in an area corresponding to a vertical angle of 45°. All angles are measured with the numeric key 5 as reference.

The merchant shall be given advice and warnings by the party supplying the PED regarding the correct installation and use of the PED.

The card issuers shall encourage the cardholders to report installations that do not provide for sufficient

privacy.

References

- [emvbook2] EMVCo: "EMV2000 - Integrated Circuit Card - Specification for Payment Systems - Book 2 - Security & Key Management".
- [iso95641] ISO 9564-1: "Banking - PIN management and security - PIN protection principles and techniques".
- [iso11568] ISO 11568: "Banking - Key Management (retail)", part 1 and part 2.
- [iso13491] ISO 13491: "Banking - Secure cryptographic devices (retail)".
- [pcidss] MasterCard/Visa: "Payment Card Industry – Data Security Standard". Identical document contents from both sources.
- [pciped] PCI: "POS PED Security Requirements Manual".
- [pcipin] MasterCard/Visa: "Payment Card Industry – PIN Security Requirements".
- [sacalgo] PNC SAC: "Recommended Cryptographic Methods".
- [sacpedrec] PNC SAC: "A Recommended PIN Management Implementation".
- [sacppl] PNC SAC: "A Recommended PPL Implementation".
- [saczon] PNC SAC: "Security requirements for cryptographic zone switching".

Glossary

AC	Application Cryptogram. The EMV card generated cryptogram used to authenticate a card based transaction.
APDU	Application Protocol Data Unit. General for data passed to and from an ICC.
CA	Certificate Authority. General for someone granting the validity of public keys.
CAM	Card Authentication Method. Authentication method for chip card, defined by EMV.
CVC	Card Verification Code. Cryptographic checksum for magnetic stripe.
CVV	Card Verification Value. Cryptographic checksum for magnetic stripe.
DDA	Dynamic Data Authentication. CAM method for ICC.
EFTPOS	Electronic Funds Transfer at the POS.
EMV	Europay, MasterCard, VISA. Normally stands for the ICC-standard set by these organisations.
ICC	Integrated Circuit Card. General for chip card.
IFD	Interface Device. General for an ICC reading device.
KMF	Key Management Facility. General for a key preparation and distribution system.
MAC	Message Authentication Code. Cryptographic check sum, calculated using a secret key.
PED	PIN Entry Device. General for a unit with a keyboard used for entering PIN. A PED has to be a tamper evident device. A separate and dedicated PED is often called PED.
PIN	Personal Identification Number.
PNC	PAN Nordic Card Association.
PNC SAC	The PNC security committee for PIN security.
POS	Point of Sale.
PPL	Program and Parameter Load. General for downloading software and parameters to a terminal.
PPL client	Function in terminal, responsible for verification of loaded items (software and parameters).
SA	Security Administrator, normally appointed by the acquiring bank.
SAC	Security Advisory Committee.
SAM	Secure Application Module. General for an application dependent security module.
SD	Secure Device. General for a secure device as defined by ref[iso13491].
SDA	Static Data Authentication. CAM method for ICC.
signing	For this document the process of making a digital signature using a cryptographic method.
SÄKO-I	Stands for Swedish Security Committee, IT. Today replaced by PNC SAC.
TMS	Terminal Management System.
TSP	Terminal Services Provider.
UKPT	Unique derived Key Per Transaction.

xPC Stands for any processing centre.