European Association
Of Payment Service Providers
For Merchants

EPSM

Point to Point Encryption and Terminal Requirements in Europe

- Status Report -

A Study for the
European Association of Payment Service Providers for Merchants EPSM

prepared by

SRC Security Research & Consulting GmbH
Graurheindorfer Str. 149 A
53117 Bonn, Germany

Bonn, 16 May 2011

Contents

Management Summary

The European Association for Payment Service Providers for Merchants EPSM asked for an overview on requirements to be supported by POS terminals in Europe with the expectation to be provided with a clear guidance how to achieve the best solution. This request is well understood, because the POS environment is one of the most challenging questions today. Especially the security programs of the global card schemes and their specification and certification organization PCI SSC lay down complex and difficult sets of requirements linked to huge investments of the acquiring markets. Due to these programs numerous new solutions emerge in the market promising to solve all challenges.

The document at hand provides the overview EPSM has asked for covering the most important sets of requirements. More sets of requirements might have been included, but looking at the selection being covered the benefit of an extension would be only marginal. In addition this document describes and assesses the most relevant vendor solutions being currently offered in the market. Both parts result in a lively and coloured status report.

EPSM's expectation on a guidance or best practice solutions to meet the requirements best, however, faces several challenges. The most important one is the lacking guidance on the interpretation and application of the different PCI standards. PCI SSC confirmed during an interview performed for this study, that it hopes to publish their guidance document "Validation requirements for P2PE solutions" in Q2/2011. This document is expected to close the gaps identified by the document at hand.

Therefore the current situation can be summarized as follows:

- The requirements to be met are numerous, complex and difficult.
- Some solutions, which are offered (and installed) today may be approached with respect since some features or requirements are critical or are not clear by now. These solutions are not as mature as they should be.
- Other solutions, which are offered (and installed) today may pass the different certification processes, but result in vendor specific dependencies.
- Investments being made today for solutions face a high degree of uncertainty and financial risks: Either they may not meet the requirements or may be too complex, i.e. too expensive.

To overcome this situation the only way forward is to wait for the guidance document of PCI SSC. The paper is expected to enter the consultation phase with the global card schemes now before being published at the end of 2Q 2011. SRC was offered to be involved. Being provided with this guidance and improved certainty further steps should be envisaged.

EPSM and its members are in an excellent position to develop an own implementation guideline or industry standard taking all requirements into consideration. An integrated and state-of-the-art-approach – which may include a few core solutions - will provide huge benefit to the payment service providers in Europe which are facing more and more requirements within the upcoming SEPA world on one hand and economic pressures on the other hand. Such an approach would also be able to reduce the complexity in many PCI DSS implementation projects not only at payment service providers but also their customers, the merchants.

For optimization purposes, EPSM should participate in the PCI SSC Special Interest Group dealing with P2PE to assure that the knowledge and experiences of the European payment service providers will be taken into account. In addition, EPSM should liaise with PCI SSC, that will develop the audit guidance for POS terminals.

Finally, it is recommended, that EPSM continues its efforts in this area and develop one or a set of P2PE implementation guidance or best practice documents with the aim to reduce the risks of not meeting all requirements and therefore of bad investments when implementing a POS approach.

1 Background and Objectives

Background

This Working Paper is sponsored by the European Payment Service Provider for Merchants (EPSM) organisation. EPSM is an interest representation and information platform of currently 60 European payment network operators, acquirers and other payment service providers for merchants. Among the non-voting members are terminal manufacturers, processing providers and payment schemes.

One of the main objectives of this community is to achieve a secure, reliable and interoperable POS terminal base. However, for different reasons POS devices are operating in one of the most dynamic and challenging markets in these days:

- The EMV migration requiring more powerful terminal hardware;
- The enduring support of the magnetic stripe technology for the acceptance of non European cards;
- The SEPA project of the European Regulators, resulting in harmonisation and convergence strategies of card schemes migrating from nationally defined security requirements;
- The new security strategy of the global card schemes, targeting at an overall protection of card data in order to face low secure environments in the “Card Not Present/e-commerce” business;

These developments resulted in a mixture of established and well known sets of security requirements mandated by the card schemes. These sets of security requirements are often not defined in an easy-implementable way. Instead, card schemes very often rely on generic requirements, which need additional implementation solutions. This is done for good reasons in order not to dictate specific implementation solutions, but to enable the vendor market to develop customised and high efficient solutions.

These separated, card scheme individual requirements now enter the phase of harmonised implementations provided by the SEPA initiative of the Open Standards for Security and Certification OSeC. This initiative simplifies the implementation, but introduces a new formal evaluation and certification methodology for POS terminals: ISO/IEC 15408, Common Criteria.

One of the most crucial challenges, however, is the overall security program of the global card schemes, published and maintained by PCI SSC. Around this program the “emerging technologies” were announced in the 2009 community meetings of the PCI SSC, which include

- end-to-end encryption,
- tokenisation,
- magnetic stripe imaging and
- virtual terminals.

In particular around the first two approaches a real hype of implementation solutions and concepts occurred within the PCI DSS stakeholder community, which see a possible silver bullet to overcome PCI DSS easily. But probably this promise may not materialise, not underestimating the potential and elegance these approaches allegedly have. As usual, the devil is in the details, and implementation requires a broad knowledge about the strengths and weaknesses of the technologies and solutions the industry has started to deliver.

The new “emerging technologies” programs of PCI SSC are still lacking implementation guidelines, which could prove for a certain level of trust and reliability. Due to their complexity and challenges for the retail environment these programs are in the focus of this document.

Objectives

Because of the situation described before, the EPSM community is confronted with a huge number of security requirements and programs, different implementation solutions evolving in the service provider and vendor markets combined with an unclear orientation for the future.

Therefore the objective of this working paper is twofold:

- first, to provide for a structured overview of the various requirements and programs a POS vendor and thus in the end the merchant currently has to consider and,
- secondly, to provide for first conclusions including critical issues detected during the collections and first analysis.

Finally next steps are proposed in order to approach the real target: Best practices for implementations, which are compliant to the security programs of the schemes and which serve the merchant community best.

Structure of the Document

This document is organised as follows:

Chapter 2 sets the scene and frames the scope of this document. In particular it will describe how to address the PCI DSS implementation in a POS retail environment. For that, the most common and typical POS scenarios are described as well as the challenges faced by the merchant.

Chapter 3 provides an overview of the different requirements of the various stakeholders involved in card payments, i.e. the card schemes and their certification bodies, e.g. PCI SSC, the former national card schemes and regulatory entities.

Chapter 4 describes the different implementation solutions defined by the market sofar including the “emerging technologies”.

Chapters 5 and 6 provide for additional information often being discussed within the framework of POS security requirements:

- the relationship of EMV and PCI DSS and
- the relationship of PCI DSS and the more and more important legal provisions of data (privacy) protection

Chapter 7 provides for a summary and a proposal for further steps how to achieve reliable implementation solutions.

2 Basic Items of Interest

The Payment Card Industry (PCI) started to design its requirements suite for secure POS terminals in the late 1990s. It started with a list of security requirements for attended POS terminals. With the decision of the global card schemes to harmonise their security and certification business by the foundation of the PCI SSC, the security programs started to emerge. The EMV implementation covered the risk of fraudulent cards being used for payment transactions in the face to face business environment. But in parallel the Card Not Present business emerged enormously where only the Primary Account Number (PAN) and the Expiry Date can be used without adequate authentication measures. (see chapter 5).

To cover the risk coming out of this environment, the PCI DSS programs were developed.

Due to the attack potential described above, the attackers‘ and criminals’ object of desire is cardholder data. By obtaining the PAN and sensitive authentication data, a thief can impersonate the cardholder, use the card, and steal the cardholder’s identity.

Acting in a hybrid environment, where EMV is more or less well-established in a still remaining wide-spread magnetic stripe environment, sensitive cardholder data can be stolen from many places, e.g.:

- Compromised card readers
- Paper stored in a filing cabinet
- Data in a payment system database
- Hidden camera recording entry of authentication data
- Secret tap into a store’s wireless or wired network

The PCI SSC has developed a series of industry standards that aim to protect sensitive cardholder data, each of it with a particular application scope:

- PCI PIN Transaction Security (PTS) aims to protect the PIN in PIN processing devices (PIN-Pads, HSMs, UPTs, SRED) of hardware and software vendors.
- PCI Data Security Standard (DSS) aims to protect sensitive cardholder data in the operational environments of merchants and service providers.
- PCI Payment Application Data Security Standard (PA-DSS) aims to protect sensitive cardholder data in payment applications of software vendors.

The implementation solution for these standards significantly depends on the intended or already established POI infrastructure by the merchant. The technical infrastructure influences significantly the effort for a PCI DSS assessment and the corresponding costs.

Due to the attack scenario PCI DSS is based on, the protection of card data is the crucial issue to decide on an implementation.

2.1 Scenarios of Merchant Solutions

The most relevant types of merchant POI infrastructures are described in this chapter. The critical existence of card data – stored, processed or transmitted - is highlighted in the different scenarios as well as the separation of the merchant’s and acquirer’s domain.

Standalone Desktop POI Terminal without any Connection to the Sale Terminal/System

If a merchant uses a standalone terminal, which is not connected to the merchant's infrastructure and does not transmit, process or store cardholder data, then PCI DSS is minimised to a few requirements.

The compliance validation of merchants will be reduced to the items listed in the PCI DSS Self Assessment Questionnaire Type B, which provides for the retention of paper reports or receipts only with cardholder data (imprint) and for standalone, dial-out terminals (connected via a phone line to the processor) with no electronic cardholder data storage.

To limit the applicable PCI DSS requirements in this way, all of the following requirements have to be met in addition:

- The standalone, dial-out terminals are not connected to any other systems within the merchant environment;
- The standalone, dial-out terminals are not connected to the Internet;
- The merchant does not transmit cardholder data over a network (either an internal network or the internet);
- The merchant retains only paper reports or paper copies of receipts with cardholder data, and these documents are not received electronically; and
- The merchant does not store cardholder data in electronic format.

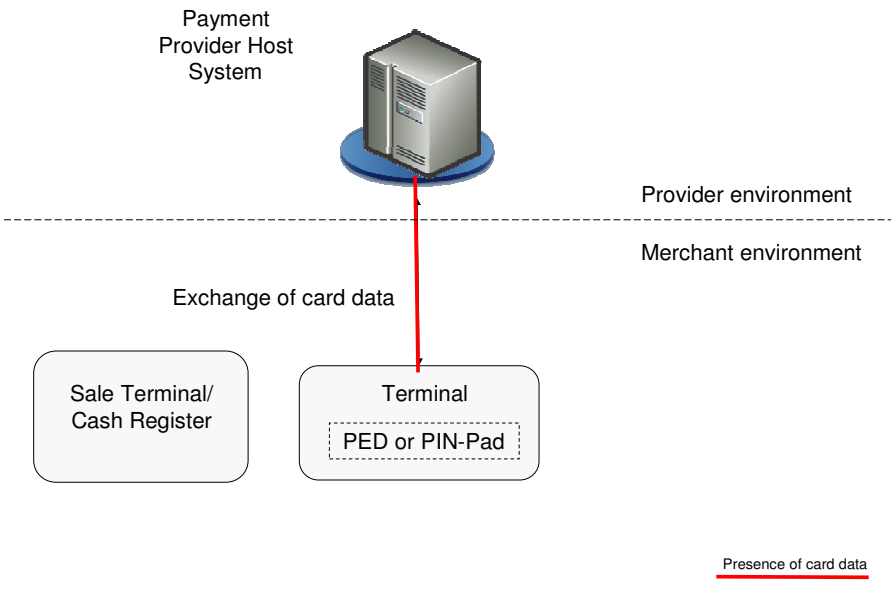


Figure 1: Standalone desktop POI terminal without any connection to the sale terminal/system

In this environment the card data are only processed by the POI terminal and the host system. The sales terminal does not get any information about the processed cards.

This document **will NOT consider this merchant solution** since the PCI DSS requirements and their validation will be applied independently of the fact whether the terminal/PIN-Pad supports P2P encryption or not. The PCI DSS compliance validation is effected by Self-Assessment Questionnaire Type A.

Connected, Integrated and/or Distributed POI Infrastructures

Accordingly, this document will only consider POI infrastructures that

- have their POS terminal connected to the retail IT environment, like e.g. sale terminal or checkout system,
- have their POS terminal connected directly to the Internet,
- transmit cardholder data over an internal network before sending it to a processor.

There are many different architectures existing in the merchant environment used for sale and payment transactions. The merchant environment mostly consists of a sale terminal or system (also called cash register) and a POS terminal (also called Point Of Interaction (POI) terminal or system in the following). The POI terminal may integrate or be connected to a PIN Entry Device (PED) also called PIN-Pad for the entry of the PIN by the cardholder. They can be categorised in :

- Connected POI terminals, means “POI connected to sale terminal”
- Integrated POI terminals, means “POI partly integrated in the sale terminal”
- Distributed POI system, means “POI functionality distributed to several components”.

Some of the most frequently used environments are described in the following:

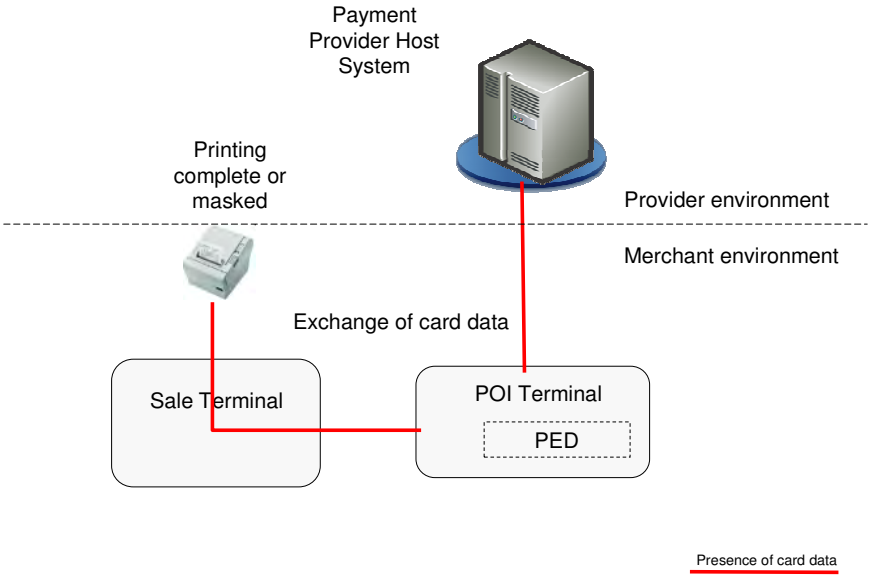


Figure 2: POI terminal connected to the sale terminal by a merchant protocol, communication with the host by the POI terminal

In this environment the card data is only provided to the sale terminal if the POI terminal delivers the card data for printing the receipt or in the payment result. If the receipt contains cardholder data resp. the full PAN (not masked) then the sale terminal will be in the scope of PCI DSS.

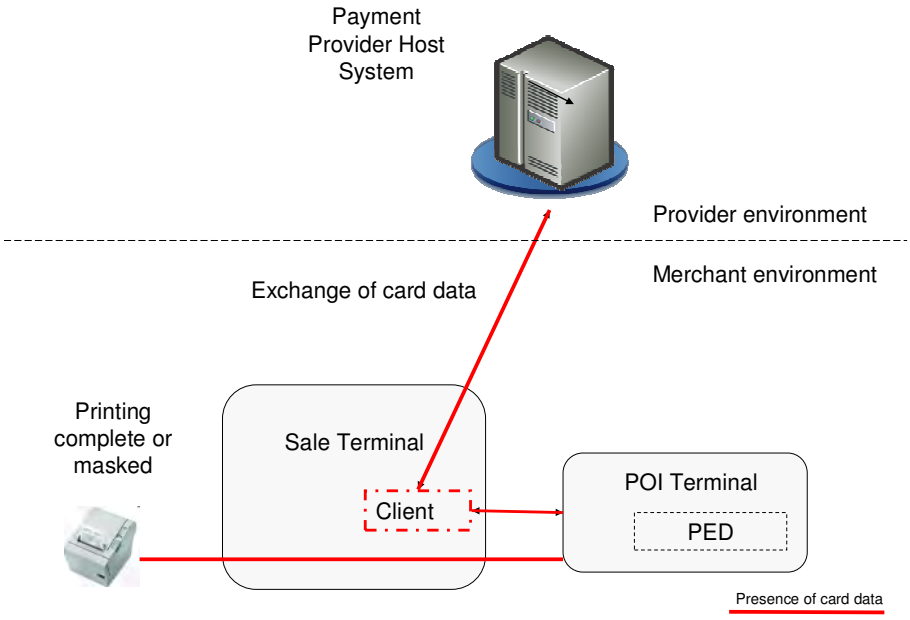


Figure 3: POI terminal connected to the sale terminal by a merchant protocol, client for the communication with the host in the sale terminal

In this environment the card data is also provided to the sale terminal if the POI terminal delivers the card data for printing the receipt or in the payment result. If the receipt contains cardholder data resp. the full PAN (not masked) then the sale terminal will be in the scope of PCI DSS.

In addition the card data is processed by the client running on the sale terminal used as communication module with the host.

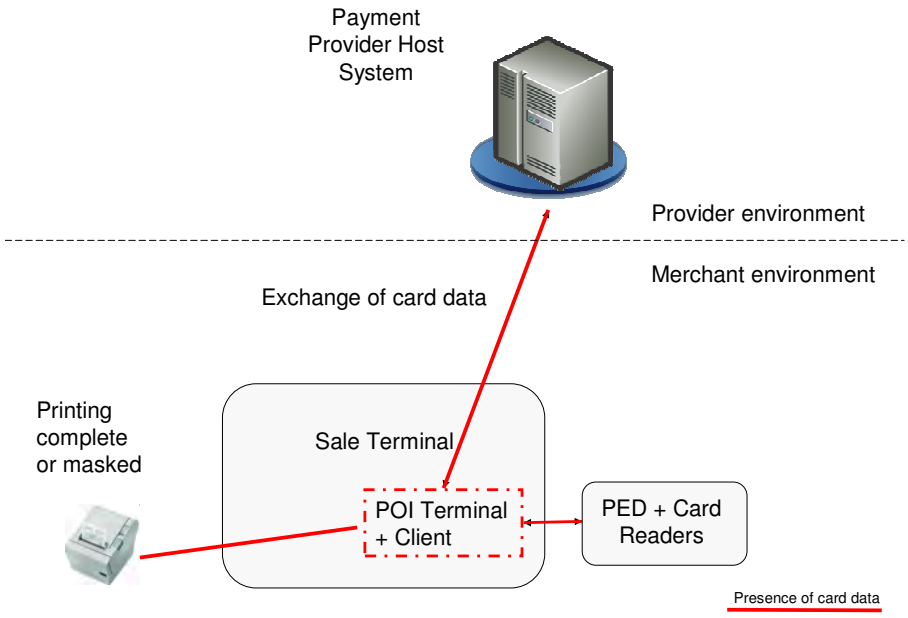


Figure 4: POI terminal integrated in the sale terminal and internally connected with a merchant protocol, the PED including the card readers are connected to the POI terminal (mostly by a serial line)

In this environment the card data is also provided to the sale terminal if the POI terminal delivers the card data for printing the receipt or in the payment result. Again, if the receipt contains cardholder data resp. the full PAN (not masked) then the sale terminal will be in the scope of PCI DSS. In addition the card data is processed by the POI terminal including the communication client running on the sale terminal and the external device consisting of the PED and the magnetic stripe as well as the ICC reader.

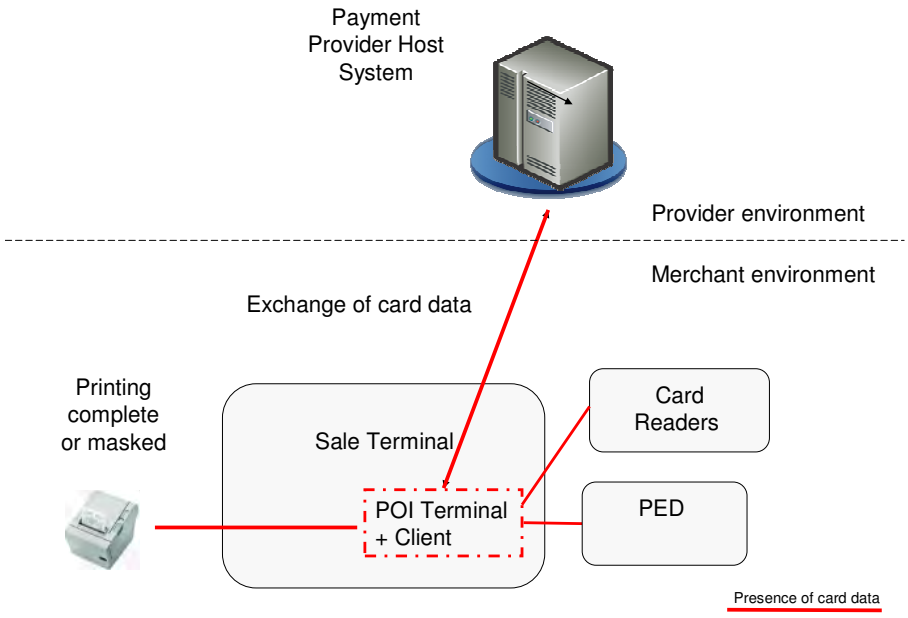


Figure 5: POI terminal integrated in the sale terminal and internally connected with a merchant protocol, the PED and the card readers are separate and connected to the POI terminal (mostly by a serial line)

In this environment the card data is also provided to the sale terminal if the POI terminal delivers the card data for printing the receipt or in the payment result. If the receipt contains cardholder data resp. the full PAN (not masked) then the sale terminal will be in the scope of PCI DSS. In addition the card data is processed by the POI terminal including the communication client running on the sale terminal and the external magnetic stripe as well as ICC reader. The PED is often used to sign the online messages so the card data is also provided to the PED.

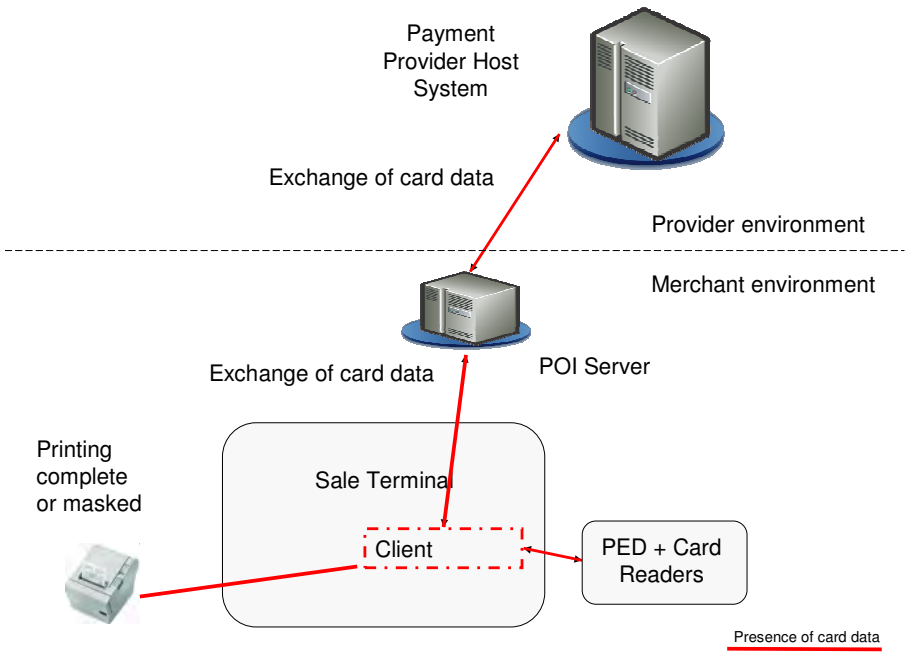


Figure 6: POI system distributed on central POI server and local client running on the sale terminal, the PED including the card readers are connected to the client (mostly by a serial line)

In this environment the card data is also provided to the sale terminal if the POI server delivers the card data for printing the receipt or in the payment result via the client. If the receipt contains card-holder data resp. the full PAN (not masked) then the sale terminal will be in the scope of PCI DSS. In addition the card data is processed by the communication client running on the sale terminal and the external device consisting of the PED and the magnetic stripe as well as ICC reader.

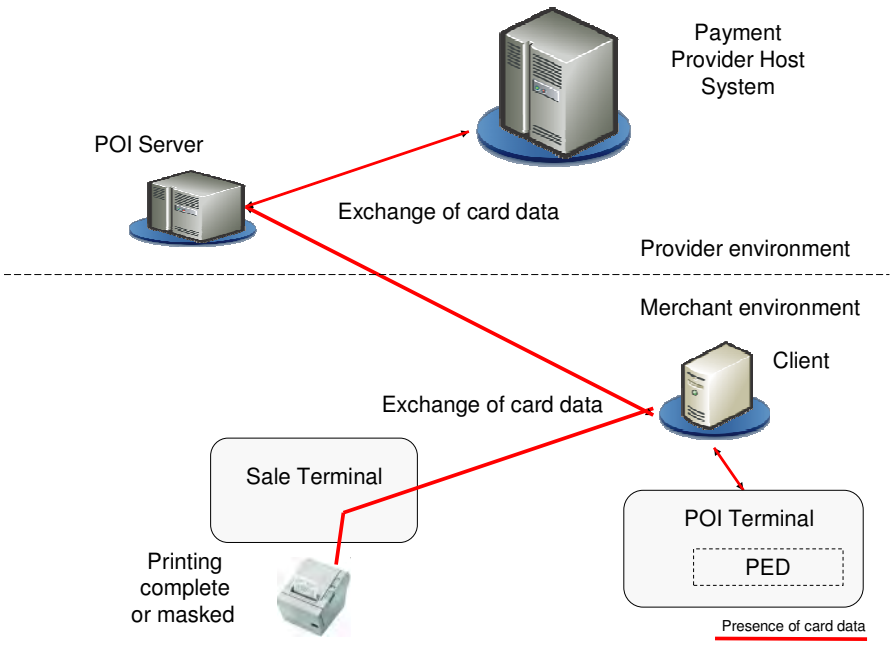


Figure 7: POI system distributed on central POI server and local client running on a dedicated system, the PED including the card readers are connected to the client (mostly by a TCP/IP connection)

In this environment the card data is also provided to the sale terminal if the POI server delivers the card data for printing the receipt or in the payment result via the client. If the receipt contains cardholder data resp. the full PAN (not masked) then the sale terminal will be in the scope of PCI DSS. In addition the card data is contained in the communication client running on the separate system and the external device consisting of the PED and the magnetic stripe and ICC reader.

Summary

In all these architectures the appearance of the card data should be minimised as far as possible. If the presence of card data is needed for the processing of the payment transaction these data have to be protected against unauthorised use.

Therefore the merchant protocol between the POI and sale system should not contain any card data except a masked PAN. The delivery of the complete card data for the printing of the cardholder and merchant receipt should be avoided.

In all communication lines between the card readers and the host system the card data have to be protected.

2.2 The Challenge: Defining the PCI DSS Scope

Having the different POI infrastructures and the PCI DSS attack potential described above in mind, the definition of the PCI DSS scope is essential. The following text summarises the main scope indications.

The Payment Card Industry Data Security Standard provides the following indications for determining the PCI DSS scope:

> *"The Primary Account Number (PAN) is the defining factor in the applicability of PCI DSS requirements and PA-DSS. If PAN is not **stored, processed, or transmitted**, PCI DSS and PA-DSS do not apply."*
>
> [Navigating PCI DSS: Understanding the Intent of the Requirements, Version 1.2, October 2008]
>
> *"The PCI DSS security requirements apply to all system components. In the context of PCI DSS, "system components" are defined as any network component, server, or application that **is included in** or **connected to** the cardholder data environment. […] The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data.*
>
> - *Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.*
> - *Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS).*
> - *Applications include all purchased and custom applications, including internal and external (for example, Internet) applications. "*
>
> [PCI DSS, Requirements and Security Assessment Procedures, Version 2.0, October 2010]

Besides in the payment processes, cardholder data is usually present in several other areas in retail environments. Cardholder data can be printed on receipts, invoices, confirmations and other customer related documents or is stored in customer relations management systems. In addition to deal with chargeback processes or requests by authorities, the merchant needs access to full cardholder data in order to prove that the card was present during the initial transaction or to reply to authorities' requests. To be compliant according to the PCI DSS, the merchant has to implement controls defined by the PCI DSS in all these areas.

In this document we will focus on the payment process only, however concepts and solutions which will be presented later may be valid in all areas cardholder data is currently stored, processed or transmitted.

It has to be noted that, in general, PCI DSS and PCI PA-DSS consider unencrypted/clear-text cardholder data and encrypted cardholder data to be the same. This means, that areas, where only encrypted cardholder data is present, is in general in scope of PCI DSS and PCI PA-DSS. However, discussions about this issue are currently not finalised. For a better understanding the following statement is cited from the FAQ article [FAQ 10359].

> *"Encryption solutions are only as good as the industry-approved algorithms and key management practices used, including security controls surrounding the encryption/decryption keys ("Keys"). If Keys are left unprotected and accessible, anyone can decrypt the data. The DSS has specific encryption key management controls (DSS 3.5 and 3.6), however, other DSS controls such as firewalls, user access controls, vulnerability management, scanning, logging and application security provide additional layers of security to prevent malicious users from gaining privileged access to networks or cardholder data environments that may grant them access to Keys. It is for this reason that encrypted cardholder data is in scope for PCI DSS."*
>
> PCI SSC FAQ, http://selfservice.talisma.com/article.aspx?article=10359&p=81

This means that any cardholder data, i.e. clear-text cardholder data as well as encrypted cardholder data, would be in the scope of PCI DSS. Applied in the context of a POS merchant, the scope would not be limited to the POS device attached to the sale terminal. In this case the scope would be much larger and would have to include all applications, systems and network components in which clear-text or encrypted cardholder data is processed, transmitted or stored, and all other systems, applications and network components, which are connected to this cardholder data environment. Therefore the cardholder data environment would easily include large parts of the whole merchant IT infrastructure.

Only under particular circumstances, encrypted cardholder data may be deemed out of scope of PCI DSS.

> *"However, encrypted data may be deemed out of scope if, and only if, it has been validated that the entity that possesses encrypted cardholder data does not have the means to decrypt it. Any technological implementation or vendor solution should be validated to ensure both physical and logical controls are in place in accordance with industry best practices, prohibiting the entity, or malicious users that may gain access to the entity's environment, from obtaining access to Keys."*
>
> PCI SSC FAQ, http://selfservice.talisma.com/article.aspx?article=10359&p=81

Accordingly, separation of encryption and decryption keys and management by different entities may offer a significant facilitation of PCI DSS implementation.

Given the definition of the cardholder data environment (see above), it is, though, not clear how this definition shall be applied in the POS context. If we consider a POS terminal as a system component similar to a PC, then the following FAQ entry provides guidance:

> *"All system components in the network are considered part of the cardholder data environment unless adequate network segmentation is in place that isolates systems that store, process, or transmit cardholder data from those that do not. Without proper network segmentation, the entire network is in scope for the PCI Data Security Standard, and all PCI Data Security Standard requirements apply."*
>
> PCI SSC FAQ, http://selfservice.talisma.com/article.aspx?article=9489&p=81

2.3 The Challenge for Merchants

The core business of merchants is to sell goods and services. Card based payments support this business. Merchants are therefore no experts in POI infrastructures and in security requirements for POI nor do they intend to become experts. Even huge department stores or forecourt stores of the petrol industry, which are equipped with IT know-how and expertise do not tend to spend too many efforts on compliance issues for their payment infrastructures.

Merchants need solutions, which are compliant and are fit for purpose. However, it is the merchants who decide which cards they want to accept at their POI. Depending on this decision, the set of security requirements to be met by the merchant's infrastructure may be different.

It is the responsibility of the card schemes, their acquirers and their acquiring technical service providers to provide for adequate information and support.

3 Requirements for POI

This chapter sums up the different security requirements mandated for POI in Europe. It is crucial to distinguish between the different mandates issued by the different card schemes. As card schemes may follow different risk strategies they can very well mandate different sets of POI security requirements.

A merchant's POI infrastructure may comply with only one scheme's requirements, if so decided, or may comply with several or all card schemes' requirements.

The following overview of the POI security requirements focus on the targets of the different sets and their individual contribution to cover the PCI DSS scope in order to provide for first insights about their "PCI DSS quality".

3.1 Requirements of the Global Card Schemes

3.1.1 PCI DSS

3.1.1.1 Overview

To encounter the increasing fraud caused by misuse of payment cards the payment schemes MasterCard and Visa have set up the programs MasterCard Site Data Protection (SDP) and Visa Account Information Security (AIS) in 2000 and 2001 respectively. Both programs seek to improve the security in the transmission, processing and storage of cardholder data.

In 2005 MasterCard and Visa joined forces and agreed upon the Payment Card Industry Data Security Standard (PCI DSS), which is today also endorsed by American Express, JCB and Discover.

The Payment Card Industry (PCI) Data Security Standard (DSS) (cf. https://www.pcisecuritystandards.org/) was introduced in September 2006 and is currently available in its latest version 2.0[1], consisting of the documents:

- Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 2.0
- Payment Card Industry (PCI) Data Security Standard - Self-Assessment Questionnaire Types A – D
- Payment Card Industry (PCI) - Approved Scanning Vendors - Program Guide Reference 1.0 - PCI DSS Version 1.2

[1] In 2011, service providers may still refer to version 1.2.1 of which the applicability will end by the end of 2011.

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to enhance cardholder data security. PCI DSS provides a baseline of technical, operational and organisational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of approximately 340 requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks.

The PCI DSS is the basis for the derived standards PA-DSS and PCI PTS (PED) which focus to applications processing cardholder data (PA-DSS) and PIN entry devices (PCI PTS).

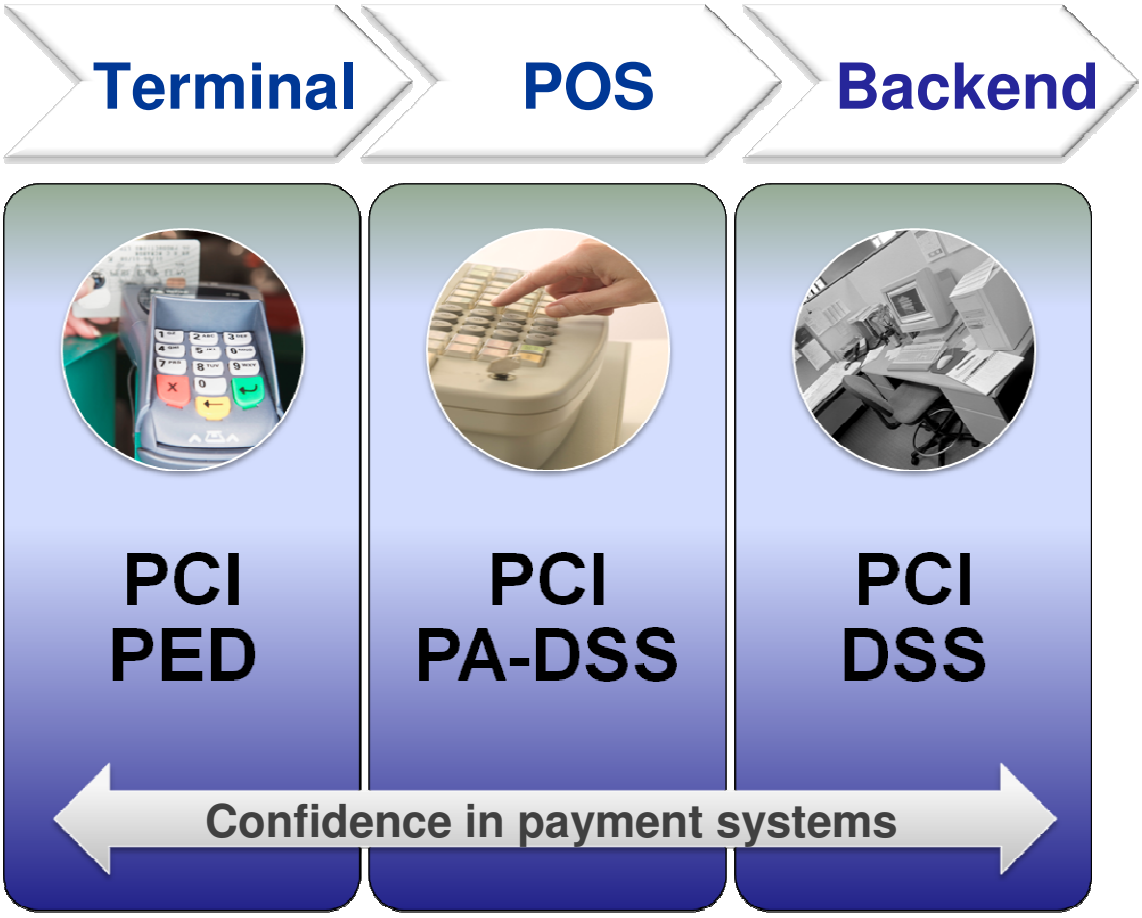
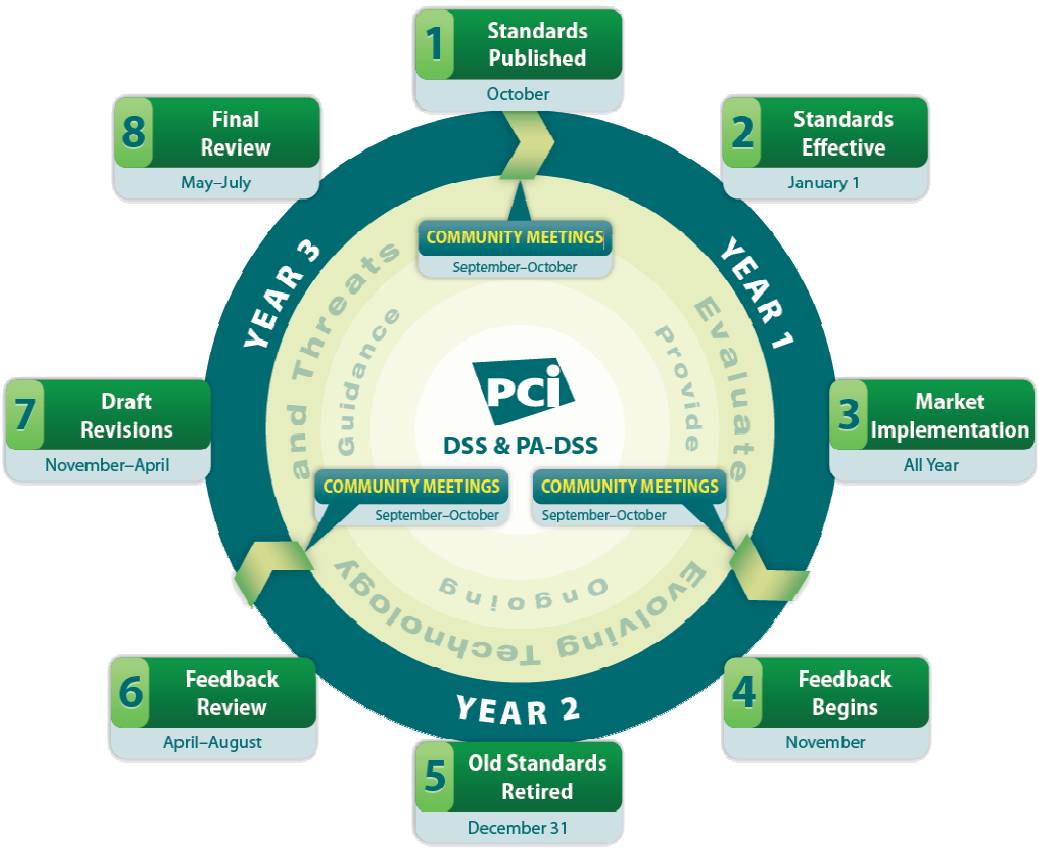


Figure 8: Overview of PCI PED, PCI PA-DSS and PCI DSS

3.1.1.2 Standard

Currently, versions 1.2.1 and 2.0 of the PCI DSS are valid (1.2.1 valid until 2011-12-31, 2.0 valid until 2014-12-31). The PCI DSS (and PA-DSS) life cycle consists of eight steps which are executed during three years.



© PCI Security Standards Council

Figure 9: Lifecycle of the PCI DSS and PA-DSS

The PCI DSS consists of 12 PCI Data Security Requirements which are structured into 6 areas:

Area 1: Build and maintain a secure network

1) Install and maintain a firewall configuration to protect cardholder data
2) Do not use vendor-supplied defaults for system passwords and other security parameters

Area 2: Protect Cardholder Data

3) Protect stored cardholder data
4) Encrypt transmission of cardholder data across open, public networks

Area 3: Maintain a Vulnerability Management Program

5) Use and regularly update anti-virus software or programs
6) Develop and maintain secure systems and applications

Area 4: Implement Strong Access Control Measures

7) Restrict access to cardholder data by business need to know
8) Assign a unique ID to each person with computer access

9) Restrict physical access to cardholder data

Area 5: Regularly Monitor and Test Networks

10) Track and monitor all access to network resources and cardholder data

11) Regularly test security systems and processes

Area 6: Maintain an Information Security Policy

12) Maintain a policy that addresses information security for all personnel

The PCI DSS consists of approximately 340 requirements in total. Every requirement includes technical measures like setting up an anti-virus system or file-integrity monitoring that must be implemented, organisational measures like roles and responsibilities that must be defined and requirements regarding documentation like written down procedures for systems management or security policies for several issues, processes like incident handling, security auditing or reporting processes, change management that includes approval management and finally tasks, that have to be carried out periodically like monthly installation of security patches or annual penetration tests.

Even while the PCI DSS consists of approximately 340 requirements, the main requirements of the PCI DSS can be summarised to the following five issues:

- Mask card number whenever possible!

  Only use first six and last four digits (e.g. 1234 56xx xxxx 3456)! This will remove areas, only masked card numbers are used in, from the PCI scope.

- Always store cardholder data encrypted!

  Whenever stored, cardholder data must be stored in encrypted form. This includes batch-processes and temporary storage!

- Access to cardholder data only on need-to-know basis!

  When humans need access to cardholder data, you have to argue why access is necessary. Therefore the number of humans having access to cardholder data must be limited.

- Log each access to cardholder data!

  Each access to cardholder data must be traceable. It must be able to identify who has access to which number of cardholder data.

- Set-up a security management system!

  A security management system including policies, responsibilities and processes must be set up and running.

3.1.1.3 Additional documents

The PCI SSC issued several supporting documents that are published on the SSC website. Besides the PCI DSS Standard, validation procedures and additional documents (supporting documents, information supplements and fact sheets) are available.

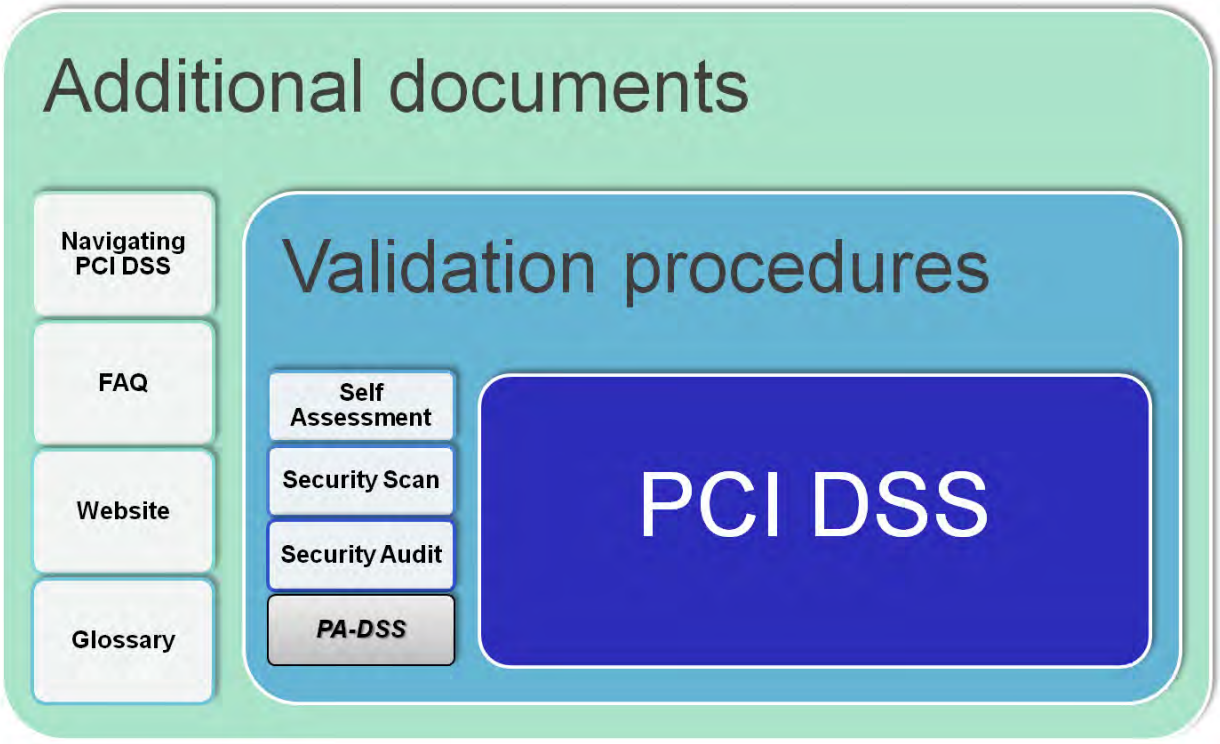


Figure 9: Overview of additional documents and information issued by the PCI SSC

The document "*Navigating PCI DSS*[2]" describes the 12 Payment Card Industry Data Security Standard (PCI DSS) requirements, along with guidance to explain the intent of each requirement. This document is intended to assist merchants, service providers, and financial institutions who may want a clearer understanding of the Payment Card Industry Data Security Standard, and the specific meaning and intention behind the detailed requirements to secure system components (servers, network, applications, etc.) that support cardholder data environments.

The Glossary[3] issued by the PCI SSC explains terms, abbreviations, and acronyms which are relevant to understand the PCI DSS.

Most important additional information is distributed via the frequently asked question (FAQ) website[4]. The FAQ is the first point of information and contains several up-to-date articles to topics of the areas

- ASV - Approved Scanning Vendor,
- DSS - Data Security Standard,

[2] https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf
[3] https://www.pcisecuritystandards.org/documents/pci_glossary_v20.pdf
[4] http://selfservice.talisma.com/display/2n/index.aspx?tab=browse&r=0.189713

- PA-DSS - Payment Application Data Security Standard,
- Participating Organisations,
- PIN Transaction Security formerly PED and
- Prioritised Approach.
- QSA - Qualified Security Assessor
- SAQ - Self-Assessment Questionnaire

3.1.2 PCI PA-DSS

The PA-DSS in general is a derivation of a “Software Standard” from the PCI Data Security Standard. Addressees of the PA-DSS are software vendors that develop systems for the processing of card data. It is the aim of the PA-DSS, that the buyer of the software shall be put in a position to be able to adhere to the PCI DSS when purchasing the software.

The PA-DSS consists of the following 14 requirements (in comparison, the PCI DSS consists of 12 requirements):

- Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2), or PIN block data
- Protect stored cardholder data
- Provide secure authentication features
- Log application activity
- Develop secure payment applications
- Protect wireless transmissions
- Test applications to address vulnerabilities
- Facilitate secure network implementation
- Cardholder data must never be stored on a server connected to the Internet
- Facilitate secure remote software updates
- Facilitate secure remote access to payment application
- Encrypt sensitive traffic over public networks
- Encrypt all non-console administrative access
- Maintain instructional documentation and training programs for customers, resellers, and integrators

The PA-DSS is applicable to any third-party payment application that stores, processes or transmits cardholder data as part of authorisation or settlement but is not applicable to self-developed software.

In POS environments the PA-DSS applies to Terminals, Cash Desks, Back-Office software that store, process or transmit cardholder data. For hardware terminals the PCI PA-DSS may not apply if all of the following items are true:

- The terminal has no connections to any of the merchant‘s systems or networks
- The terminal connects only to the acquirer or processor
- The vendor provides secure remote:
  - Updates
  - Troubleshooting
  - Access
- Maintenance
- Sensitive authentication data is never stored after authorisation

3.1.3 PCI PTS 3.0

For device vendors and manufacturers, the PCI Security Standards Council (SSC) provides the PIN Transaction Security (PTS) requirements, which contain a single set of requirements for all personal identification number (PIN) terminals, including POS devices, encrypting PIN-Pads and unattended payment terminals. The PTS security program documentation is available on https://www.pcisecuritystandards.org. The current version 3.0 of the PTS program will be mandated in April 2011.

Although the PCI PTS program is focussed on PIN security the program also includes the protection of the account data and thus brings the POI into the PCI DSS umbrella.

Replacing the formerly existing different terminal type specific requirements suits of PCI the new PTS 3.0 requirements integrate these different programs following a modular approach.

The requirements are divided in several evaluation modules. The core requirements are mandated for all devices supporting PIN transactions except software modules developed for a “open protocol handling”.

3.1.3.1 PED

For the integration of a PED and card reader in a POS terminal, especially in an Unattended POS Terminal (UPT), the module “integration requirements” have to be met.

In the core physical requirements of section A of PCI PTS, version 3.0, the requirement A10 enforces hardware security protection of the magnetic stripe reader. A11 requires "It is not feasible to penetrate the device to make any additions, substitutions, or modifications to the magnetic-stripe reader and associated hardware or software, in order to determine or modify magnetic-stripe track data….".

3.1.3.2 SRED

The “Secure Reading and Exchange of Data (SRED)” module is addressing the support of secure encryption of account data in the terminal. The SRED requirements have to be met if the vendor is declaring this security feature in the evaluation form. How the SRED certified product will be integrated in the PA DSS and PCI DSS process has still to be clarified by the PCI SSC.

In the account data protection section K of PCI PTS, version 3.0, the requirement K3 enforces the account data encryption by a cryptographic key which is protected by a hardware security device

(K3: "Determination of any cryptographic keys used for account data encryption, by penetration of the device and/or by monitoring emanations from the device (including power fluctuations), requires an attack potential of at least 26 for identification and initial exploitation with a minimum of 13 for exploitation….")

Public keys used for account data encryption must be stored and used in a manner that protects against unauthorised modification or substitution.

3.1.3.3 Open Protocols

If the POS terminal supports IP connections to open protocols (Internet, GPRS etc.) the requirements of the module “Open Protocols” have to be met.

The Open Protocols requirements in section F-J of PCI PTS, version 3.0, are based on the MasterCard PTS requirements, November 2007, for IP-enabled terminals. This set of requirements should ensure that payment devices using open security and communication protocols to access public networks and services do not have public domain vulnerabilities. The requirements focus on all supported

- IP and Link Layers,
- IP Protocols (TCP/IP, WIFI, GPRS etc.),
- security protocols (e.g. SSL, TLS) and
- IP services (e.g. DNS, DHCP, HTTP, FTP)

as well as the Security Management services for the administration of the hardware, firmware and software platform. The assessment of the device includes the analysis of the protocol stack and penetration tests/scans of it's interfaces.

3.2 Common Approval Scheme CAS / Open Standards for Security and Certification OSeC

Common Approval Scheme CAS

CAS is an international industry initiative of the European and global card schemes and approval bodies. The initiative developed a harmonised set of security requirements for POS terminals, which covers all PCI POS PED 2.1 requirements and – because of the limited scope of the PCI requirements - additional requirements, which are state of the art in Europe to protect assets beyond PIN and magnetic stripe data. This list was adopted by the EPC for publication in the SEPA Cards Standardisation Volume / Book of Requirements as a fundamental cornerstone for the harmonisation of security requirements for POS terminals to establish the SEPA for cards. The CAS list does not include new security requirements not being implemented in Europe today.

CAS established a technical expert group called JTEMS JIL Terminal Evaluation Methodology Subgroup, which transferred these requirements into three different Protection Profiles, which were certified according to the ISO 15 408 Common Criteria by the French CC Certification Body ANSSI. These profiles ensure a common, harmonised implementation of each requirement. As a result each security requirement of the common set is implemented and evaluated in the same way; enabling certifications of these evaluations to be accepted by several approval bodies for approval. Each requirement therefore needs to be evaluated only once for multiple approval (one stop shopping).

The three Protection Profiles provide for three different risk strategies ("PP comprehensive" supports the whole set of requirements and is therefore acceptable for approval by PCI oriented schemes and all others; "PP option" does not cover the protection of the magnetic stripe data and the plaintext PIN and is therefore acceptable for schemes being further evolved to a chip only environment; "PP PED" only covers the PCI POS PED 2.1 requirements and is acceptable for schemes, which follow the PCI requirements set only).

It is up to the card schemes and approval bodies to mandate the JTEMS implementation specifications for approval. The card schemes will select subsets according to their risk strategies. The three PPs described above are a starting point covering the main risk strategies currently in use.

The scope of the CAS/EPC requirements is limited to the POS terminal without its network or acquirer context. Account data protection is covered by

- Requirement A11 of the physical security requirements, which requires the protection of the magnetic stripe data.
- Requirement G1, which requires, that
    - the terminal must have the capacity to protect all transaction data sent or received by the POI against disclosure, meaning that the POI security components must provide cryptographic means to support that requirement (requirement G1.1),
    - the transaction/accounting data shall be handled with authenticity and integrity in the POI (Requirement G1.2),
    - the POI management data must be provided to the POI in an authentic way and must be protected against unauthorised change

Open Standards for Security and Certification OSeC

OSeC means Open Standards for Security and Certification. The OSeC Steering Committee is comprised of global and European Approval Bodies[5] in order to coordinate pilots of CC evaluations and certifications based on the JTEMS Protection Profiles to achieve the acceptance of these certifications by all participating approval bodies. For the pilots all security requirements of the CAS/EPC list will be covered and the "PP Comprehensive" will be used. Thus the above mentioned requirements to protect account data, magnetic stripe data, transaction data and management data will be covered.

The OSeC Steering Committee defined an overall pilot phase of 2 years (October 2010 to October 2012) which vendors can use to perform the evaluations, certifications and approvals. The first pilots start in January/February, 2011; the first certifications and approval are expected by the end of 2011.

Due to the migration to PTS 3.0 requirements, which will be effective from 1 April 2011 onwards, the OSeC Steering Committee agreed on workarounds to enable also PTS 3.0 certifications out of the CC certified JTEMS documentation.

[5] The participating card schemes and approval bodies are American Express, Cartes Bancaires, Consorzio Bancomat, Currence, The UK Card Association, The PAN Nordic Card Association, Visa Europe, MasterCard and Zentraler Kreditausschuss ZKA

3.3 Zentraler Kreditausschuss ZKA / ZKA Approval Scheme

3.3.1 girocard Requirements

Zentraler Kreditausschuss ZKA, which functions as the umbrella of the four German Credit Sector Associations administrating the girocard debit scheme (see http://www.zentraler-kreditausschuss.de/) does not define any requirements to protect card data.

ZKA requires PIN protection and the integrity of the payment system as such. Being limited to face-to-face payments girocard does not provide for a possibility to misuse pure card data since the physical card and the PIN of the cardholder have to be present for an authorisation. Card Not Present transactions are not possible within the girocard scheme.

The ZKA Approval Scheme for girocard POI is based on the Debit/Credit POS terminal specification (DC POS) and the Terminal Type Approval Interface (TAI) specification, which is a common specification of ZKA administrating the girocard debit scheme and the acquirers of the global card schemes in Germany.

3.3.2 ZKA Approval Scheme

The ZKA Approval Scheme is an Approval Scheme integrating the approval requirements and processes of the girocard debit scheme and the acquirers of the global card schemes being active in Germany.

The acquirers – in contrast to the girocard scheme – are obliged to comply with the PCI requirements.

The common Debit/Credit POS terminal specification requires that the PAN of Track 2 has to be stored in an internal journal for each approved, declined or aborted transaction, if it has been retrieved from the card. Which chip data have to be present in the journal can be defined by configuration. The access to the journal has to be limited to authorised entities only. How this protection is realised is out of scope of the ZKA approval scheme.

The POS terminal specification and TAI are defining the masking of the PAN on cardholder and merchant receipts and the configuration of this feature per card application.

The TAI online interface does not include any card data encryption mechanisms.

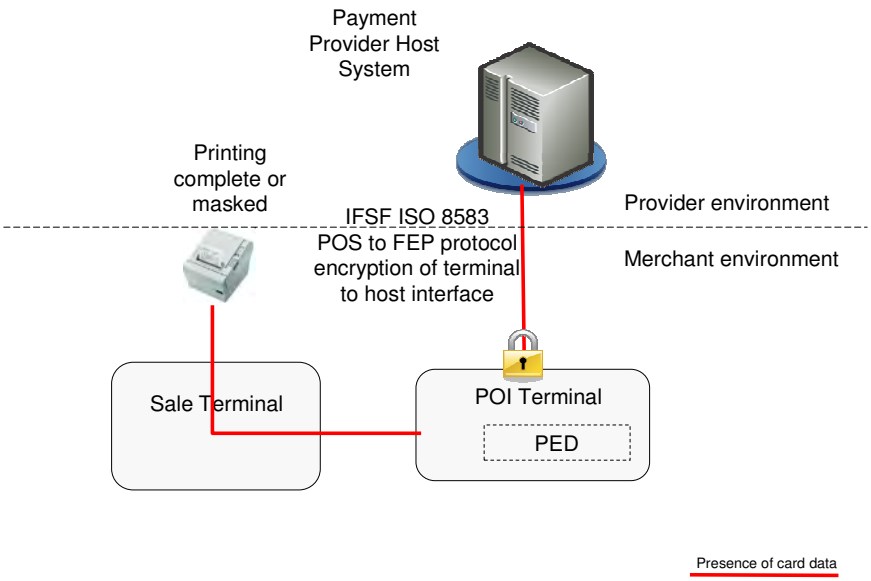
4 Solutions

Facing the introduction of PCI DSS and the other PCI security programs, different solutions were and are being developed by the market. In the following paragraphs an overview is given to selected approaches.

4.1 IFSF

The IFSF (International Forecourt Standards Forum) is a forum of international petroleum merchants with the common objective of harmonisation of communication standards for use in the petroleum retail business (see http://www.ifsf.org). The standards developed by IFSF are available for IFSF members and associates only.

IFSF has developed a set of specifications for the POS (Point of Service) to EPS (Electronic Payment Server), POS (Point of Sale –Terminal) to FEP (Front End Processor) and Host to Host interface. The POS to EPS protocol uses the XML coding. The POS to FEP and Host to Host interface are based on ISO 8583:1993 format.



IFSF is developing also recommendations for the security and key management standards of the POS to FEP and Host to Host interfaces.

Part of the recommendations is the Format Preserving Encryption (FPE) algorithm; a technique for encrypting sensitive data in a manner that preserves the format of the original data, e.g. the result of encrypting 10 decimal digits would still be 10 decimal digits.

The FPE algorithm is foreseen for the encryption of the card data in the online messages in order to meet the PCI DSS requirement.

There are two modes of the FPE:

- encryption of the sensitive data by hardware security modules (hardware mode);

the encryption of the data by the sender is performed before generating the MAC of the complete message or

- encryption by software modules (software mode);

  the encryption of the data by the sender is performed after generating the MAC of the complete message

In hardware mode of the POS to FEP interface the PIN-Pad will be used to encrypt the data using a new variant of the DUKPT key. The FEP is using then the Host Security Module (HSM) for the decryption.

In hardware mode of the HOST to HOST interface the HSMs will be used to encrypt and decrypt the data using a new variant of the master session key derivation.

In software mode of the POS to FEP interface a software security module will be used by the terminal to encrypt the data. The cryptographic keys are stored in the application of the POI terminal or server.

The encryption is performed by the sender of a message after the MAC generation. The receiver of the message has to decrypt the message elements containing FPE data and to replace the corresponding data elements of the message by the plain text before verifying the MAC of the message.

4.2 EPAS

Introduction

The EPAS protocols are a set of specifications for the exchange of card-based transactions between a merchant (Acceptor) and an Acquirer.

The EPAS Acquirer Protocol, EPAS Terminal Management System (TMS) Protocol and the EPAS Merchant Protocol are developed by EPASOrg, an international non-profit association whose aim is to develop specifications for card-based payment and non-payment transactions. EPAS protocols are open, royalty-free, and ready for implementation.

The EPAS Acquirer Protocol is already integrated in the ISO 20022 standards and published on http://www.iso20022.org/UNIFI_Cards_messages.page.

The EPAS Terminal Management System (TMS) is drafted and will be published on ISO 20022 in the beginning of 2011.

The first version of the EPAS Merchant Protocol is available for free to any interested party on http://www.epasorg.eu

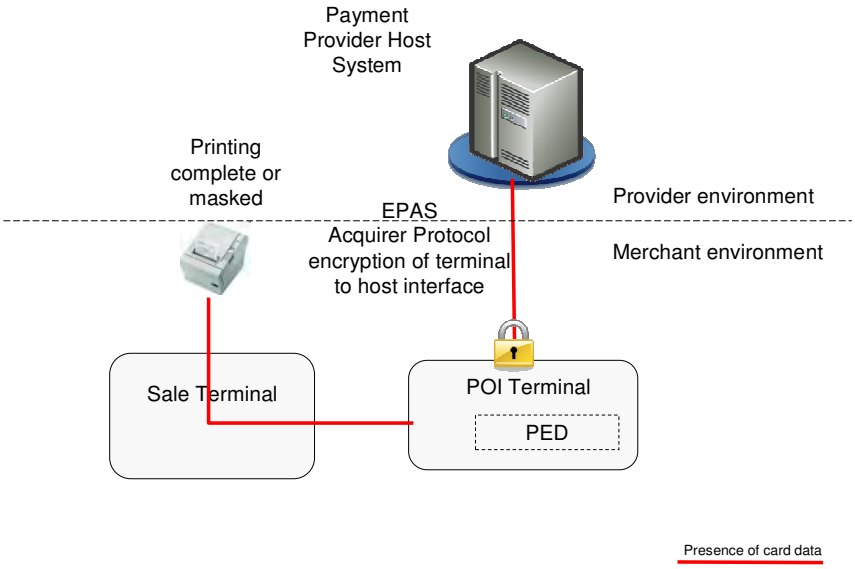
The version 1.0 of the EPAS protocols is available in XML coding. The functionality of the EPAS Acquirers and EPAS TMS Protocol is specified in the Message Definition Report (MDR) that is part of the ISO20022 documentation and the Message Usage Guide (MUG) available on EPASOrg.eu. The EPAS Merchant Protocol specification has not been submitted to ISO 20022 and includes the data dictionary and XML Schema directly.

Account Data protection of the Acquirer Protocol

The EPAS standard supports protection mechanisms on the application layer. Security services of the transport protocol or session layer (e.g. SSL/TLS) are not part of the specification.

The message elements of the Acquirer Protocol containing card related data (PAN, Expiry data, Track 1 and Track 2 etc.) can be sent in plain (message component *PlainCardData*) or encrypted (message component *ProtectedCardData*).

The *ProtectedCardData* is formatted in a Cryptograhic Message Syntax (CMS) structure. This CMS structure contains all information the recipient needs to identify and derive the cryptographic key and the used algorithms. The EPAS Acquirer protocol version 1.0 supports the Triple-DES encryption of the complete card data message component (PAN, expiry date, Track etc.) using the Derived Unique Key Per Transaction algorithm (DUKPT) or the Master Session key algorithm for key derivation as well as the RSA encryption of the transport key.



In principle the EPAS Acquirer Protocol security mechanisms can use separate keys and algorithms for each cryptographic function of the protocol. In the MUG of the protocol three variants of the DUKPT key are recommended as key derivation for the PIN encryption, MAC generation and data encryption function between a terminal and a host.

For the EPAS Acquirer Protocol the initiator of a message encrypts the card data before generating the MAC.

In the response message the card data message component is optional. If the protected card data are present this message component is a copy of the data sent in the request.

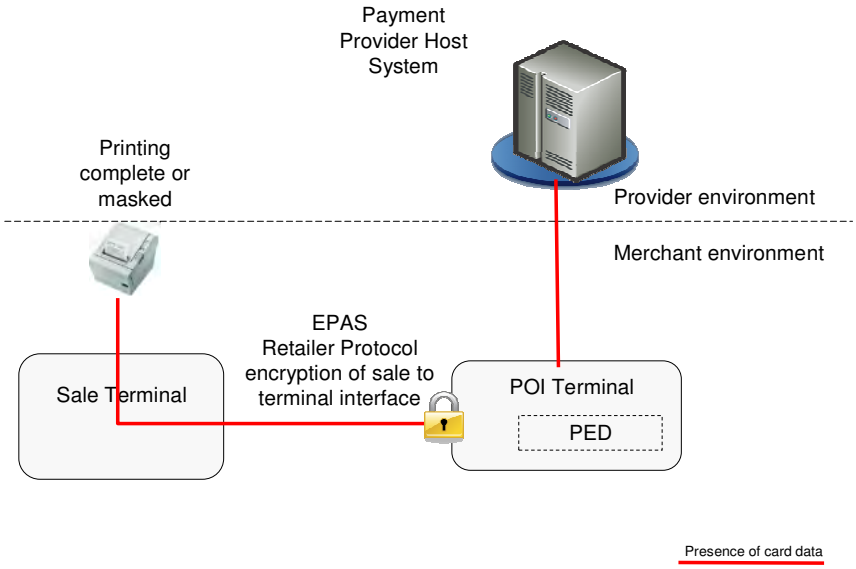
Account Data protection of the TMS Protocol

The EPAS TMS Protocol does not contain any card data. In the configuration parameters for the POI application there is an indicator per Acquirer identification whether the card data have to be protected or not. This indicator is used to replace the message component *PlainCardData* of the Acquirer Protocol request as well as response message by the *ProtectedCardData*.

Account Data protection of the Merchant Protocol

The standard payment services and also the device services (display and printer output) of the EPAS Merchant Protocol may contain card data.

In the Payment request message of the sale system (work station or electronic cash register) the manually entered card data can be delivered to the POI in plain text or encrypted. The encrypted card data are transported in a CMS structure. The version 1.0 of the merchant protocol supports a Triple DES encryption with a transport key encrypted with a master key. The master key has to be installed in the sale and POI system.



In the Payment Response message the card data may be present in plain text, encrypted or in parts (e.g. only the masked PAN is sent, neither Track data nor the expiry date of the card are present).

In the device services of the POI sent to the sale system for receipt printing any card data can be present according to the implementation of the payment application of the POI. If the POI is implemented according to the SEPA-FAST specification (see SEPA-FAST) the cardholder and merchant receipt can be configured in a way that only the masked PAN is printed.

4.3 Common Implementation Recommendations CIR/Open Standards for Cards OSCAR

Common Implementation Recommendations CIR

The CIR (Common Implementation Recommendations) Technical Working Group is an open standardisation initiative of EMV implementers in Europe and acts as the technical reference group for the European EMV Users Group and the European members of the EMVCo Board of Advisors (see www.cir-twg.org).

The CIR-TWG delivered the first common standard for payment terminals, the "Financial Application Specification for SCF Compliant EMV Terminals" (SEPA-FAST). SEPA-FAST is based on

EMV Chip and PIN technology and describes unambiguously the financial application on a terminal which is compliant to the SEPA Cards Framework (SCF).

SEPA-FAST will be delivered in three parts:

- Part 1, for the Attended POS Environment
- Part 2, for the Unattended POS Environment
- Part 3, for the ATM

In addition a specification for the Contactless interface will be issued.

Version 1.00 of Part 1 has already been published. Part 2 and Contactless are in progress and will be published in 2011.

SEPA-FAST consists of:

- The detailed technical specification of the functions, processing steps, display messages and receipts needed to perform Card Services
- A top-level flow describing each of the Card Services and detailed flows describing the functions and processing steps needed to process the Card Services
- The Data Dictionary giving the technical description of the data elements used in the technical specification

The online messages to the Acquirer host and the interface to the sales system are not part of the SEPA-FAST specification. This functionality is described in a generic form as Host Application Protocol (HAP) and Sale System Protocol (SaSP).

SEPA-FAST Part 1 does not describe the internal protection of the card data by the terminal during the processing flow. But a PAN Mask can be configured for the truncation of the PAN on the cardholder as well as merchant receipt. The mask consists of a leading and a trailing part. Digits that are not indicated to be printed according to either the Leading PAN Mask or the Trailing PAN Mask will be replaced by the character "x".

Open Standards for Cards OSCAR

The OSCar project coordinates a field trial for the implementation of SEPA-FAST and EPAS specifications involving interested vendors, payment service providers, merchants and card schemes. The pilot will be conducted in a multi-scheme and multi-country context. It will demonstrate the viability of the SEPA terminal concept compliant with the SEPA standards, certified once and used in different SEPA countries for different schemes.

The implementation of SEPA-FAST and EPAS-specifications are combined in an integrated specification, so that terminal vendors and payment service providers are able to develop POS applications and acquirer systems.

In addition the OSCar Consortium will define the OSCar certification policy and test cases allowing a detailed functional test and a certification by the involved certification bodies.

The scope of the OSCAR project is limited to the services payment, cancellation and refund defined in SEPA-FAST Part 1 using the EPAS Acquirer protocol messages for authorisation as well

as cancellation and the EPAS TMS protocol for the download of Acquiring parameters. The implementation of the EPAS Merchant Protocol will be optional for the vendors to ease the function test.

The mechanisms of SEPA-FAST Part 1 for PAN masking on the receipts and the card data encryption in the online messages will be part of the functional test validation.

4.4 PNC

The PNC PCI DSS compliance program (see www.pan-nordic.org) requires that all POS have to fulfil End-to-End Encryption according to "Visa Best Practice Data Field Encryption, Version 1.0" and have to be PA-DSS certified by a PA-QSA.

The acquirer protocol specifications and Sales system to POS terminal protocol specification for an Integrated Point of Sale (iPOS) are not public.

4.5 Emerging Technologies@POS/Approaches

Tokenisation and encryption are two different methods to replace valuable PANs by not valuable information. Encryption is a process that transforms the sensitive information (plaintext, here the PAN) using an encryption algorithm (cipher) and a secret (called key) to an unreadable information (called ciphertext). Decryption is the reverse process transforming the ciphertext to plaintext using the key. Tokenisation is a process that replaces the sensitive information (here the PAN) to a unique but random value (called the token). The tokens are usually stored[6] in a mapping table beside the original value.

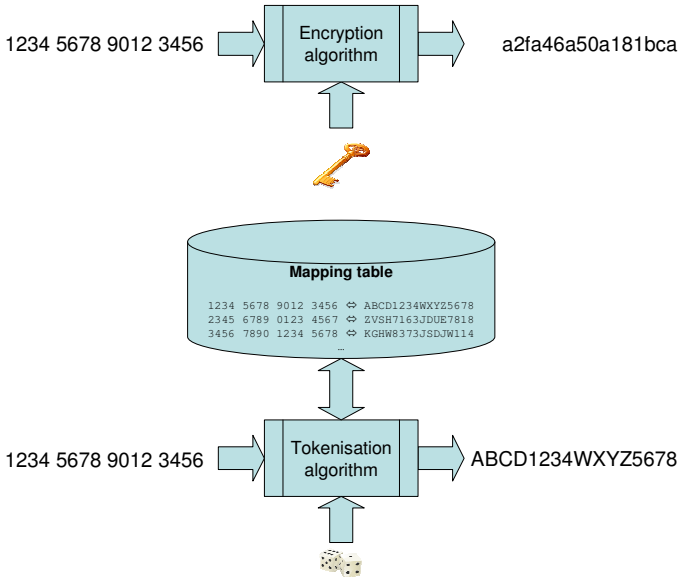


Figure 10: The process of encryption and tokenisation

[6] If the original value is a PAN, it must be stored encrypted according to PCI DSS requirements.

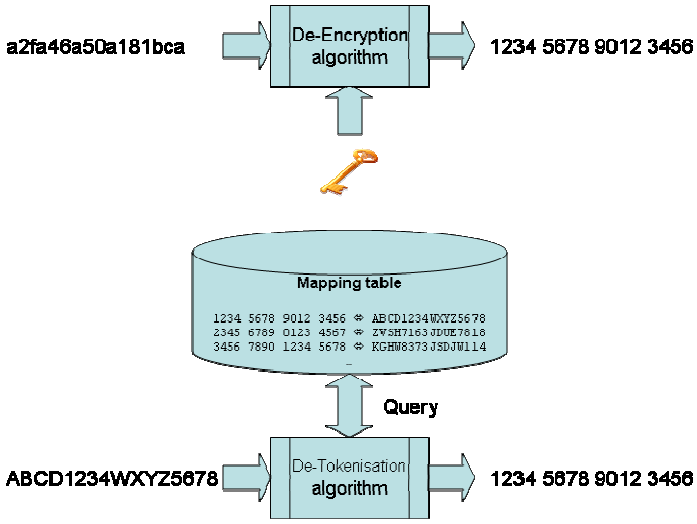


Figure 11: The process of decryption and de-tokenisation

From the security point of view the major difference between tokenisation and encryption is the fact that for encryption one single encryption key must be kept secret. For tokenisation a whole mapping table must be kept secret. In both cases the secret part (cryptographic key and mapping table) must be kept secret.

4.5.1 Tokenisation

The term “tokenisation” is used for a technology that replaces a unique PAN to another unique value. From the experience of various projects it is known that the PAN is used in several business processes and applications without necessity. The idea of tokenisation is that the PAN is replaced by unique “tokens” in such business processes and/or applications. The goal of “tokenisation” is to keep areas in which cardholder data is not needed out of PCI DSS scope. This will limit the effort to implement PCI DSS.

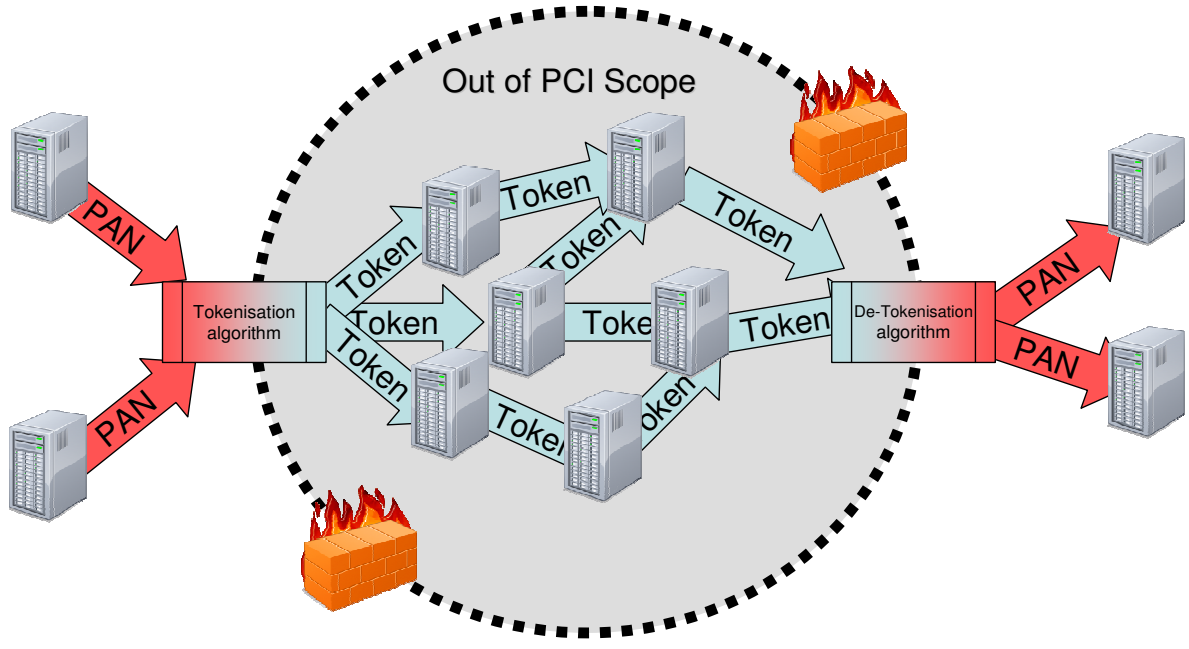


Figure 12: Principle of Tokenisation

4.5.2 Point-to-Point Encryption

The document [PCI-P2PE] discusses encryption solutions and how those solutions may simplify compliance efforts within the PCI Data Security Standard. It is obviously true that encrypted data (like the sensitive cardholder data, CHD) is well protected as long as the used cryptographic key will not become public. For this reason the PCI SSC has clarified that encrypted data is out of scope of the PCI DSS only if the entity possessing the encrypted CHD does not have the means to decrypt it (cf. [FAQ 10359]).

The current discussion in [PCI-P2PE] refers exclusively to the *transmission* of PCI DSS relevant card data. Statements regarding a processing or storage of encrypted data are not made in this document, however. Within the above-referenced entry of the FAQ one can find the following statement:

> "... *Encrypted data may be deemed out of scope if, and only if, it has been validated that the entity that possesses encrypted cardholder data does not have the means to decrypt it."*
>
> PCI SSC FAQ, http://selfservice.talisma.com/article.aspx?article=10359&p=81

Based on this statement of the FAQ also stored and processed encrypted card data can be taken in/out of scope ? of the PCI DSS. Therefore it might be expected that the document [PCI-P2PE] will be expanded in future and that precise demands on the storage and processing of encrypted card data will be defined.

The current discussion allows the following statements regarding the requirements for encrypted card data:

1. The encryption of PCI DSS relevant card data must be performed in a certified environment. Requirements will be defined in the previously undisclosed document "Validation Requirements for Point-to-Point Encryption".
   In the present case, this means that systems (e.g. POI) - in which the encryption is carried out – have to undergo an appropriate certification process.
2. For the handling of cryptographic keys (key management) strict rules have to be defined.
3. The entity, which performs the decryption, must satisfy the requirements of the PCI DSS.

Regarding storage and processing of encrypted card data it can be referred to the above mentioned entry in the FAQ of the PCI SSC. The application of this interpretation allows, that even by storing and processing of encrypted card data, the related components are not subject to the PCI DSS requirements, until there are specific instructions of the PCI SSC. Especially in batch processes, in temporary off-line cases, this interpretation may be helpful. For the sake of completeness it must be mentioned that this interpretation is not covered within [PCI-P2PE].

The current state of the discussion does not allow a reliable statement with regard to the question, how to deal with encrypted card data around PCI DSS in future. In particular it is currently unclear, whether and - if yes - how to deal with processed or stored encrypted card data and whether the storing / processing component is subject to the requirements of the PCI DSS. The current documentation only specifies the requirements for the transmission of encrypted data.

The PCI SSC has already announced the "*Validation Requirements for Point-to-Point Encryption*". The contents of the document is not known so far. The publication of the document has been announced for the second quarter of 2011.

4.5.2.1 Symmetric and asymmetric encryption

In general two different encryption methods are distinguished: symmetric and asymmetric encryption.

The main difference between both methods is the way how the cryptographic keys are handled. While symmetric cryptographic systems are characterised by using the same key for encryption and decryption, the keys in asymmetric systems are different. Moreover in an asymmetric system one of the keys could be made public – in symmetric schemes the key has to be protected and kept secret all the time. This property has a strong impact on the management of the keys. It is not possible (in terms of probability as long as the key length is sufficient) to decrypt a message which was encrypted using a public key unless you are in the possession of the private key.

The algorithms itself are in all cases publicly known, validated by a strong scientific community and can be implemented either in software or in hardware. The secret lies always in the key.

Examples for symmetric algorithms are Triple-DES (Data Encryption Standard) or AES (Advanced Encryption Standard) and for asymmetric algorithms RSA (named after the inventors: Rivest, Shamir and Adleman) or ECC (short for Elliptic Curve Cryptography).

In all cases the length of the keys correlates to the security of a system. For symmetric algorithms the key must be so long that at least a brute force attack (that means searching over the whole key space) would take such a long time, that even in case of success the result is worthless. The single DES has a key length of 56 bit which is regarded nowadays as too short. The Triple-DES variant with two keys has 112 bit key length, with three keys 168 bit and the AES is standardised with 128 bit, 192 bit and 256 bit.

Nowadays, within the credit industry the two key Triple-DES is used. Some governmental institutions have published documents saying, this key length will no longer be regarded as secure in the near future.

The EMV Standard has introduced RSA as a cryptographic technique for authentication between card and payment terminal and as a secure means to transmit a PIN encrypted to the smartcard. As an international industry standard the only acceptable way to store keys within every terminal sofar was through the usage of asymmetric public key cryptography. EMV has now published versions of the specifications, which describe the usage of AES and Elliptic Curve Cryptography.

4.5.2.2 Key Management: PCI PIN Security Requirements

In close relationship, every encryption solution has to resolve the corresponding problem of key management . This means that the decision for encryption of sensitive date like CHD or SAD (sensitive authentication data) and the selection of a cryptographic algorithm (realised in an appropriate

device e.g. SRED or POI) is not sufficient for the design of a 'good' encryption system. In addition a thoroughly designed key management has to be introduced to achieve this goal.

The authors of [PCI-P2PE] were aware of this, because within the document it is mentioned several times that a separate document describing *validation requirements* for Point-to-Point encryption will follow. So on the one hand – without having such a document – for any implementation of an encryption scheme (not meeting the requirements in [FAQ 10359]) the achievement of PCI compliance or an answer to the question, if a specific part is out of scope of the PCI DSS could only be decided case to case. On the other hand the payment industry has solid experience in using cryptographic techniques at least for the encryption of PINs for authorisation within online transactions. In this connection also key management issues have been solved. Key management is especially addressed and plays a major role in [PCI PSK]. Due to that fact chapter 6.2.3 in [PCI-P2PE] reflects to these requirements and they should be regarded as a sound basis for the *validation requirements* which have to be developed by PCI.

In general, any Key Management concept has to specify how cryptographic keys are

- generated,
- distributed,
- stored,
- accessed,
- used,
- destroyed,
- archived

and how this life cycle is documented and controlled.

At least the generation and distribution of keys seems to be solved in “Identity Based Encryption (IBE) schemes” which are provided by some payment service providers (see chapter 4.6). Such schemes – first introduced by Shamir in 1984 ([Shamir84]) which could be regarded as specialised versions of a public key encryption system – allow the usage of an identity as a public key. So data encrypted with such a key cannot be decrypted, not even by the sender, and will therefore be out of scope for the PCI DSS. One has to be aware that the implementation of such IBE-schemes requires the existence of a trusted third party for the provision of the secret keys which is therefore definitely within the scope of PCI DSS.

4.5.2.3 Secure Channel: VPN, TLS (Server authentication, C/S authentication)

As a main part within the security conception it must be decided – and no general strategy exists – at which communication level the encryption is introduced. It is of course always possible to encrypt the data which are affected by the PCI DSS on application level. This might probably not be a flexible solution since if further data have to protected (if the DSS requirements change or due to further requirements) the application must be changed, which is expensive and time-consuming in case of peripheral applications. The encryption of the whole communication link (using TLS and client server authentication) might be more practical in such cases. Nevertheless it has to be checked, where the encryption in such a design ends and if the data are handled in the intended way.

PCI addresses the requirements within the PCI PTS 3.0 standard. It was discussed in chapter 3.1.3.3, that “open protocols” like TCP/IP, TLS, IPSec, etc have to be assessed e.g. by analysis of the protocol stack and penetration tests/scans of the devices’ interfaces. From the point of view of the PCI SSC all aspects are considered since requirements on all levels have to be respected to achieve a coherent and complete picture of a secure processing of cardholder data.

4.6 Industry Solutions

4.6.1 Heartland Payment Systems E3Secure

Heartland Payment Systems delivers credit/debit/prepaid card processing, gift marketing, payroll, check management and related business solutions to more than 250,000 business locations in North America. The E3Secure solution is a point-to-point encryption product by Heartland Payment Systems which implements a solution as described in the PCI SSC document "*Initial Roadmap*: Point-to-Point Encryption Technology and PCI DSS Compliance”. E3Secure is designed to protect credit and debit card data from the moment of card swipe or key entry — and through the Heartland network — not just at certain points of the transaction flow. The main characteristics of the E3Secure systems are (according to [E3_TAWP])

- Hardware Based Encryption when the transaction is swiped or key entered (POI)
- Use of a PTS validated terminal
- Encryption hardware and encryption key material protected by a tamper resistant security module (TRSM)
- Unique encryption keys for every encrypting device deployed
- Frequent changing of the encryption keys
- Decryption keys are never exposed to merchants and only available to their Acquirer

The statements with respect to key management are made because E3Secure supports identity based encryption.

4.6.2 Verifone VeriShield Protect

VeriShield Protect is a solution that provides merchants with strong encryption of payment card data from the point of capture to the point of transmission of the encrypted data to a network operator or processor.

Verifone VeriShield Protect builds upon a patented technology called VeriShield Hidden Encryption (VHE), a format-preserving encryption (FPE) method that encrypts the primary account number and discretionary data so that most other applications interpret the data as valid card data. VHE is able to encrypt only a part of the card data while retaining the first six (BIN) or the last four numbers (including the Luhn check digit) of the PAN unencrypted, so that a change in the POI payment application can be avoided in most cases. Also, encrypted card data is formatted in a way that e.g. a Luhn check on the data including the encrypted data will work.

Also format preserving has several advantages when processing or storing encrypted data like PANs there might be a disadvantage with respect to PCI audit requirements: if the Luhn check digit is preserved there is at least a 10% chance that a format preserved encrypted PAN will again result in a valid PAN. To confirm the accuracy and appropriateness of PCI DSS scope, an auditor has to perfom the following:

- The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE) (see [PCI DSS, page 10])

Therefore it is an open question how an auditor or forensic investigator that is looking for PANs e.g. to determine the scope of PCI DSS can separate original PANs from FPE generated PANs.

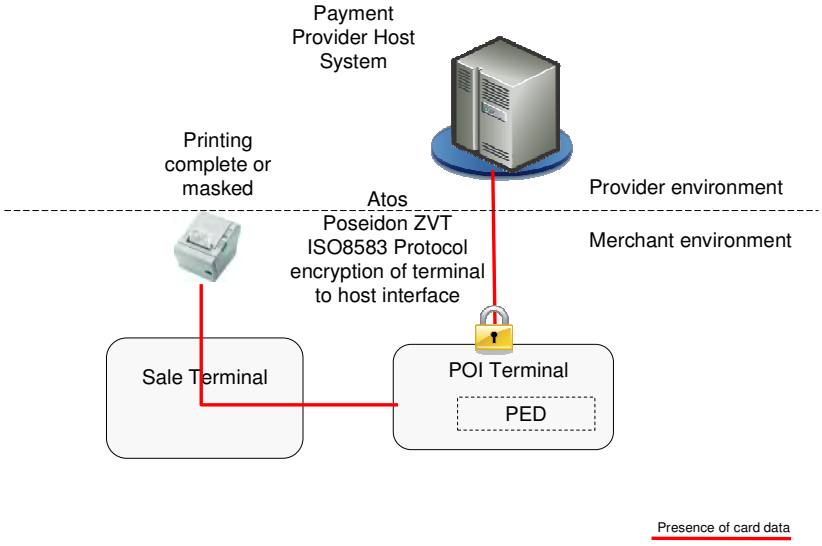
The FPE is implemented as an encryption mode of the Advanced Encryption Standard (AES). The encryption is performed in a Tamper Resistant Security Module (TRSM) of a terminal which is certified according to FIPS 140 Level II at the minimum.

4.6.3 ATOS Worldline

ATOS Wordline as supplier for electronic transaction processing offers card data protection mechanisms integrated in the ISO8583 terminal interface to the payment provider host called POSEIDON ZVT:

- BMP-Encryption and
- E2EE (End to End Encryption)

These solutions have been presented during the POSEIDON-ZVT info forum in Oct. 2010.



For the BMP-Encryption of the ISO8583 data elements the terminal software uses it's hardware security module (PED, card reader or separate HSM) to encrypt directly the relevant elements of the online messages after generating the MAC. The provider host software decrypts the card data using the Host Security Module and verifies the integrity subsequently. In this case the card data in clear are available in the terminal application, the HSM of the terminal and the host application including the HSM.

In the E2EE solution the security module of the terminal encrypts directly the card data of the online messages. The encrypted data are placed in a separate element of the online message (BMP 48). The BMP 2 of the message contains only the prefix of the PAN for routing purposes if necessary. In this case the data are not available in clear in any POI terminal or server application. The provider host checks the integrity of the message including the encrypted card data and decrypts the dedicated message element using the host security module.

5 PCI DSS and EMV

The card payment markets invested a huge amount of money into the chip migration of their infrastructures during the last years. According to statistics published by the EPC the EMV migration is coming to an end in Europe – just inline with the targets of the SEPA Cards Framework, requiring the support of EMV/IC technology until the end of 2010. As the improvement of card payments' security was the goal of the EMV migration, one could ask, why the PCI SSC security programs are necessary in addition. Therefore PCI SSC in 2010 published the document [PCI EMV], explaining the benefits of EMV and PCI DSS and the necessity to implement both sets of requirements.

The main arguments are summarised as follows:

- EMV targets to prevent the risk of transactions with fraudulent cards providing cryptographic means in order to ensure secure authentication of the card in face to face payments. Using PIN as CVM – EMV is providing for several usage options - the risk of lost and stolen fraud can be limited to a minimum in addition. Experiences show, that these goals are achieved.
- EMV, however, was never intended to protect authorisation and cardholder data against unauthorised access. PAN and Expiry Date are processed in clear text. These data can therefore be compromised in the still existing magnetic stripe environment in order to be misused for fraudulent transactions in badly protected "Card Not Present" (CNP) environments, where it is sufficient to get an authorisation based on these limited data.

As explained in chapter 3.1.1 PCI DSS is designed to close this gap. It aims at component integrity and at card data confidentiality in case of reading, storage, processing and transmission. The PCI SSC approach looks at all hybrid and magnetic stripe only ATM or POS and their processing infrastructures as potential Points of Compromise, which can be counteracted by adequate PCI DSS implementations.

It is clearly said in [PCI EMV], that its DSS program is needed as long as the face-to-face payment infrastructure is still supporting the magnetic stripe and "unsecure" authentication processes can be used for CNP transactions, especially in e-commerce. In an EMV-only environment and a CNP environment equipped with reliable authentication features, PCI DSS needs reconsideration.

6 PCI DSS and Data Protection

In 1995, the European Union released Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. More commonly known as the European Data Protection Directive, this directive forms the principles for the protection of personal data within the EU. As with any directive of the European Union, the Data Protection Directive is not legally binding for citizens of the EU, but had to be adopted into national law by all member states of the union. Directive 95/46/EC therefore does not regulate the protection of private personal data within the EU, but lays the fundamental ground for member states to achieve their own privacy protection legislation, offering them certain leeway regarding the concrete design of their individual law.

6.1 Data Protection Act in EU

The Data Protection Directive defines the minimum standard of data protection that every Member State of the EU has to ensure by national law. This alignment of national data protection legislation is to prevent restrictions of data transmission between different Member States due to different levels of privacy, thus fostering the free flow of data within the EU.

The Directive derives a person's right to data protection from the fundamental rights and freedoms of natural persons, especially the right to privacy. Thereby, the data protection regulation set out in the directive is directly linked to natural persons. Accordingly, personal data is defined as "any information relating to an identified or identifiable natural person". Identifiable means that the person "can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his […] identity" (95/46/EC Article 2 (a)). By this definition, data is considered as personal data if a possible link to the relating person exists, no matter whether the holder of data himself can conduct this connection. Therefore, also credit card numbers or other banking card data that can theoretically be traced back to the person can be considered as personal data in terms of the Data Protection Directive.

The processing of such personal data is strictly regulated by the Data Protection Directive and thereby by all derived national laws. In this context, "processing of data" is to be understood as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" (95/46/EC Article 2 (b)). The person or institution establishing the purposes and means of the processing of personal data is called the controller of data. It can be noted that the directive's definition of processing is rather broad and does not only cover automated, but also manual means.

By article 7 of the directive, all member states are bound to prohibit any such processing of data unless

- the person the data is related to (the "data subject") has given his/her consent or
- the processing is necessary for
    - the performance of / the entering into a contract,
    - compliance with a legal obligation,

- the protection of the data subject's vital interests,
- a task carried out in public interest or in the exercise of official authority,
- the legitimate interests pursued by the data controller (weighting to respecting the interests for fundamental rights and freedoms of the person) (95/46/EC Article 7).

Meeting the above listed criteria is essential for the legitimacy of any collection or processing of personal data. In addition, the Data Protection Directive specifies several conditions that have to be met in order to ensure a fair and lawful processing.

One of the key principles of legitimate data processing according to Directive 95/46/EC is the concept of the specified purpose. Personal data shall be collected and processed only for specified, explicit and legitimate purposes. Any processing that goes beyond the specified purpose shall be prohibited. Furthermore, the processed data shall be relevant for the specified purpose, and shall be accurate as well as up-to-date. If it is no longer necessary for the purpose, the data shall not be allowed to be maintained any more (95/46/EC Article 6).

Whenever personal data is collected from or about any data subject, he/she shall be informed about this specified purpose. In addition, the data subject shall be informed about the identity of the data controller, the recipients of data, and his/her right to access and amend the data concerning him/her (unless the storage or disclosure is expressly required by law). He/she shall be allowed to access this information, plus the information which data has been collected and where it came from, in appropriate intervals without exceeding delay or expenses. As data shall be accurate, the person also must be allowed to amend his/her personal data (95/46/EC Article 10, 11, 12).

In order to ensure appropriate protection of personal data, data controllers shall be required to take technical and organisational measures suitable for protection of the personal data against

- accidental or unlawful destruction,
- accidental loss,
- unauthorised alteration,
- unauthorised disclosure or access and
- any other unlawful forms of processing.

The level of protection should be adequate considering state of the art best practices and standards of protection, the kind of data, the risks processing it, and the costs for protection. If processing personal data is delegated to an external processor, the data controller is responsible to make sure that the external processor provides a sufficient level of protection, and only processes the data as directed by the controller (95/46/EC Article 17).

As these principles of collecting and processing personal data have to be adopted by all member states of the European Union, it is assumed that a comparable level of privacy protection is present in all member states. Therefore, the transmission of personal data inside the EU is subject to different requirements than transmission to countries outside the EU. According to the Data Protection Directive, data transmission to countries outside the EU ("third countries") is only allowed if they provide an adequate protection level. If a country cannot assure such a protection level, the controller has to make sure the foreign processor himself guarantees sufficient protection of privacy, freedoms and the exercise of associated rights, e.g. by appropriate contract terms like the ones recorded in 2010/87/EU ("Commission Decision on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council").

6.2 Example: Data Protection Act in DE National Requirements

While the European Data Protection Directive provides the ground for data protection legislation within the European Union, it is not legally binding for EU citizens but had to be put into national legislation in every Member State. In Germany, the Federal Data Protection Act ("Bundesdatenschutzgesetz", BDSG) got adjusted to the European Data Protection Directive in 2001. In 2009, the BDSG has been amended by three separate enactments of the German Parliament. Changes introduced by the amendment include new legislation regarding scoring, credit enquiry agencies and revised duties to furnish information, especially in the case of compromise of credit card or account information.

Since the amendment in 2009, § 42a BDSG includes provisions for notifications in the case of data breaches. If a data controller discovers that third parties have unlawfully obtained knowledge of sensitive personal data (including banking and credit card data), and serious damage for the rights or interests of the relating data subjects is imminent, the following actions have to be taken:

- taking of adequate measures for the protection of the data;
- immediate notification of supervisory authority;
- immediate notification of persons whose personal data is affected, or, if that would require excessive expenses, of the public via at least half-page announcements in two nationally published newspapers

This mandate for notification of persons affected by a data breach resp. of the public is not derived from the European Data Protection Directive. Even though the BDSG includes several exigencies that go beyond the mandates of the directive. German legislation in general follows the principles of the Data Protection Directive. § 4 BDSG provides the need for specified and legitimate purposes set out by article 6 of Directive 95/46/EC. § 3a BDSG amends an obligation of anonymisation or creation of pseudonyms whenever possible. The directive's parameters regarding information and access are transferred to, amongst others, § 4 BDSG. For example, § 4 (3) BDSG lays down that the person of whom data is collected, stored or disclosed must be informed by the data controller about

- who is the controller of the collected data;
- what is the purpose of data processing;
- who else will receive this data (if the person cannot face it from the circumstances).

The necessity to take adequate technical and organisational measures for the protection of personal data is set out in § 9 BDSG. In addition, the appendix to § 9 BDSG names the following principles for the protection of personal data

- Admission control: only authorised persons shall have admission to data processing equipment used for the processing of personal data;
- System access control: only authorised persons shall be able to use data processing systems;
- Data access control: persons authorised to access processing systems shall only be able to access data they are authorised for;
- Transmission control: there shall be a warranty that data cannot be read, copied, modified or deleted during transmission;
- Input control: there shall be logging measures in place to determine who did enter, modify or delete data;
- Order control: there shall be a warranty that external parties processing personal data by order only do so in the way directed by the controller;
- Availability control: there shall be measures in place to provide protection against destruction by accident or loss;
- Segregation control: there shall be measures in place to ensure that data that has been collected for different purposes can also be processed separately.

The BDSG does not provide any further information on how to achieve the goals set out by these eight principles. However, it does specify that the measures shall be suitable to achieve an adequate level of protection and that measures are only necessary when the effort is appropriate with regards to the intended purpose.

6.3 ISO 27001/2 and PCI DSS as Implementations

To determine adequate controls with regard to the data in question, the underlying risks against said data and the necessary effort of implementing measures, established security standards and security best practices such as ISO 27001 / ISO 27002 or PCI DSS can be used.

While the ISO 27001 provides an abstract framework for a top-down approach, deriving security measures on the basis of a risk assessment, the PCI DSS is a more concrete standard. It comprises a collection of concrete requirements for the protection of cardholder data. As the PCI DSS is an established standard for the protection of sensitive data being tangent to all eight data protection principles described above, it can be used as a basis for selecting appropriate controls to fulfil the BDSG's mandate for adequate technical and organisational measures.

It can be expected that an implementation of PCI DSS has a positive emanation effect on other personal data within it's scope, therefore supporting the adherence to data protection regulation regarding technical and organisational measures. Furthermore, measure-driven standards such as the PCI DSS can be used as a collection of best practices; the application of selected PCI DSS controls can help in achieving a baseline security level for system environments outside the PCI DSS's original scope.

7 Open Issues

This report shows that there is certain degree of complexity to develop a suitable and appropriate P2PE approach meeting today's (unclear) requirements and exploiting the potential P2PE undoubtedly has. In addition, not all requirements are clear or not defined yet.

In particular, there are some critical questions which need to be answered in the P2PE context.

First, there are questions around the Format Preserving Encryption which, at least partly, replaces original PANs with new PANs that are the result of a format preserving encryption operation. It is an open question how an auditor or forensic investigator that is looking for PANs e.g. to determine the scope of PCI DSS can separate original PANs from FPE generated PANs.

Second, it is not clear how the scope of a sale terminal to which a P2PE enabled PIN-pad is attached (either by USB, serial) or an IP-based P2PE enabled PIN-pad which is connected to a network is determined. Does e.g. a PCI PTS 3.0 validated PIN-Pad in which a hardware security module stores the cryptographic keys used in the P2PE constitute a PCI scope on its own, or does the scope include also the sales terminal to which the PIN-Pad is attached or the networks segment in which the PIN-pad is located?

Third, it remains unclear whether the endpoints of a P2PE solution require secure hardware support e.g. by a PCI PTS approved PIN-pad or Common Criteria EAL4+ evaluated and certified hardware security module, or whether a software solution implemented would be acceptable provided that the system on which the software runs is protected by PCI DSS itself?

And finally, the minimum requirements for the cryptographic protocols of a P2PE solution are not clearly defined yet.

These are some questions that call for clarification before a P2PE solution that realizes the potential benefits is designed and implemented.

It is hoped that the document "Validation requirements for P2PE solution" which is expected to be released end of Q2/2011 by PCI DSS shall provide the guidance and missing information required to develop a robust and state-of-the-art P2PE solution.

8 About SRC

SRC is an independent consultancy company that was founded in 2000 by the German banking industry as the joint centre of excellence for card-based payments and IT security.

SRC is a widely recognised and well respected company with experienced and highly skilled employees, some of whom have been working as IT security consultants for more than twenty five years. SRC's mission is to become the leading consulting company when it is about products and services around the creation, implementation and operation of secure systems – for the banking industry, financial institutions or insurance companies, the retail sector, public services or manufacturers. SRC's professional services organisation offers a wide variety of consulting, training and deployment support to its customers.

As an independent consultancy, SRC supports its customers in any question concerning card payments and IT security, and thus designs, specifies, develops, evaluates, and certifies security applications in general, and in the areas of electronic payment transactions, chip card-, e- and m-commerce, as well as digital signatures or the security of computer networks in specific.

Already in 2003, SRC was the first company worldwide to successfully complete the process of accreditation with both MasterCard and Visa. Since then, SRC is authorised to conduct security assessments on behalf of the payment schemes.

SRC was the first company worldwide [7] that was awarded with accreditations as

- PCI Qualified Security Assessor (PCI QSA),
- PCI Approved Scanning Vendor (PCI ASV),
- PCI Payment Application Qualified Security Assessor (PCI PA-QSA)
- PCI PIN Transaction Security testing lab (PCI PTS lab)

by PCI SSC.

SRC is authorised by MasterCard to perform audits that evaluate compliance with MasterCard Security Requirements for Mobile Provisioning, also referred as Over The Air Personalisation.

SRC is an accredited "Logical Security" and "Physical Security" auditor for the assessment of plastic card personalisation companies within in the MasterCard Global Vendor Compliance Program.

[7] See: http://www.pcisecuritystandards.org/

9 References

[PCI DSS] Payment Card Industry Data Security Standard, Version 2.0, October 2010, Payment Card Industry Security Standards Council

[PCI EMV] PCI DSS Applicability in an EMV Environment – A Guidance Document, Version 1, 5 October 2010, Payment Card Industry Security Standards Council

[Visa DFE] Visa Europe's Best Practices for Data Field Encryption, Version 1.0, Visa Europe

[Visa DFE DKM] Visa Europe Data Field Encryption: Device and Key Management Guidance, Version 1.0, March 2010, Visa Europe

[MC E2EE] An Analysis of End-to-end Encryption as a Viable Solution for Securing Payment Card Data, October 2009

[PCI-P2PE] Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance, PCI Security Standards Council, Emerging Technology Whitepaper, October 5, 2010

[FAQ 10359] Article # 10359 on the PCI-SSC FAQ website

[PCI PSK] Payment Card Industry: PIN Security Requirements, Version 2.0, January 2008

[E3_TAWP] Heartland Payment Systems E3™ Terminal Technical Assessment White Paper, Coalfire, 5.11.2010

[Shamir84] Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7, pp. 47--53, 1984

[VERIFONE] VeriShield Description, http://www.verifone.com/sites/verishield-protect.aspx accessed on 22 February 2011