FORWARD THINKING IT SOLUTIONS

WHITE PAPER

Security for Card-Based Transactions

V1.1

1 Abstract

This whitepaper gives an overview over the wide field of Security Technologies for Card-Based Transactions. Along the chain of communication starting with payment cards, proceeding via payment terminals, ATMs, payment service providers, acquirers, payment networks ending at your issuing bank, communication of sensitive payment and customer data needs to be thoroughly protected by adequate security technology.

With over 25-years experience in various aspects of securing card-based transactions we show the actors involved and the needs of them in their security environment. Based on international and country-specific security standards we depict how Ergonomics can help in implementing a secure solution.

2 Surrounding Field / Actors / Vendors

A card-based transaction starts at the point of sale (POS) or at an automated teller machine (ATM). The cardholder inserts the card and enters the PIN. The terminal sends a request with the encrypted PIN and encrypted sensitive cardholder data to the acquirer. The acquirer translates the PIN and routes the request to the responsible issuer. The issuer authorizes the transaction and responds to the acquirer. The acquirer routes the response back to the terminal.

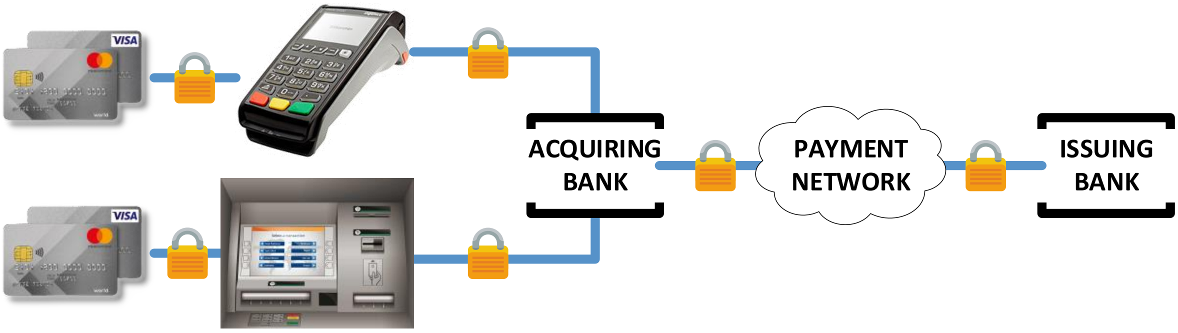

Figure 1 Secure communication in financial payment card networks, involving payment cards, payment terminals or ATMs, acquiring banks, payment networks, and issuing banks.

Involved Party	Remarks
Merchant	The merchant needs: • a terminal with a compliant EPP (Encrypting PIN Pad) that stores secret keys and allows secure PIN entry • a compliant secure process for loading the keys (shared with the acquirer) into the EPP • a software on the terminal that takes care of issuing the correct commands to the EPP (probably also an EMV chip, if one is involved), encrypting the sensitive cardholder data and communicating with the acquirer • a compliant secured connection to the acquirer
Acquirer	The acquirer that connects the merchant to the issuer needs: • a compliant HSM (hardware security module) that stores secret keys and supports PIN translation (decrypting PIN with terminal key and encrypting PIN with issuer key) • compliant secure processes to share keys with terminals and issuers • a service listening to terminal requests, issuing the correct commands to the HSM and routing the request to the responsible issuer • compliant secured connections to the terminals and the issuers
Issuer	The issuer of the card that authorizes the transaction needs: • a compliant HSM that stores secret keys and supports PIN decryption (with keys shared with the acquirers) • a compliant secure process to share keys with the acquirers • a service listening to acquirer requests, issuing the correct commands to the HSM and authorizing the request (probably with additional help of other background services) • compliant secured connections to acquirers and background systems
HSM Vendor	The HSM vendor has: • compliant HW • compliant firmware on the HW that supports the necessary functionality for acquirer and/or issuer systems
EPP Vendor	The EPP vendor has: • compliant HW • compliant firmware on the HW that implements the CEN/XFS interface • a compliant process for initial loading of the keys into the EPP (factory key loading) • a compliant process to exchange credentials with the acquirer

Table 1 Involved parties

3 Overview Security Standards

One of the most important organizations regarding security standards for card-based transactions is the PCI (Payment Card Industry) organization PCI SSC (PCI Security Standards Council), which has been founded by American Express, Discover, JCB International, MasterCard and Visa.

PCI SSC publishes among others the following PCI security standards:

- PCI PTS (PCI PIN Transaction Security Requirements) is focused on characteristics and management of devices used in the protection of cardholder PINs and other payment processing related activities. Manufacturers must follow these requirements in the design, manufacture and transport of a device to the entity that implements it.
- PA-DSS (Payment Application Data Security Standard) is for software vendors and others who develop payment applications that store, process or transmit cardholder data and/or sensitive authentication data, for example as part of authorization or settlement when these applications are sold, distributed or licensed to third parties.

The PCI security standard documents base upon other international standards like:

- ANSI X9.24, Retail Financial Services Symmetric Key Management
  standard that deals with symmetric key management techniques for retail financial services
- ANSI X9.73, Cryptographic Message Syntax – ASN.1 and XML Standard
  specifies a cryptographic syntax scheme that can be used to protect financial transactions, files, and other messages from unauthorized disclosure and modification
- ANSI X9 TR31, Interoperable Secure Key Exchange Key Block Specification
  Key Blocks have been invented as a standard way for protecting the integrity of symmetric cryptographic keys and for identifying what the keys can be used for.
- ANSI X9 TR34, Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques
  describes a method consistent with the requirements of ANS X9.24 for the secure exchange of keys using asymmetric techniques between two devices that share asymmetric keys
- ISO 9564, Financial services — Personal Identification Number (PIN) management and security
  international standard for personal identification number (PIN) management and security in financial services
- ISO 9797, Information technology — Security techniques — Message Authentication Codes (MACs)
  international standard that defines methods for calculating a message authentication code (MAC) over data

These standards in turn refer to other international standards like:

- RFC 2315, PKCS #7, Cryptographic Message Syntax
IETF's standard for cryptographically protected messages. It can be used by cryptographic schemes and protocols to digitally sign, digest, authenticate or encrypt any form of digital data.
- RFC 2985, PKCS #9: Selected Object Classes and Attribute Types
Defines selected attribute types for use in PKCS #6 extended certificates, PKCS #7 digitally signed messages, PKCS #8 private-key information, and PKCS #10 certificate-signing requests.
- RFC 2986, PKCS #10, Certification Request Syntax Specification
Format of messages sent to a certification authority to request certification of a public key. See certificate signing request.
- RFC 3560, RSAES-OAEP in CMS
conventions for using the RSAES-OAEP key transport algorithm with the Cryptographic Message Syntax (CMS)
- RFC 5280, X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) standard defining the format of public key certificates

Beside of these international standards, there exist also country-specific standards, like:

- The standards published by the German Banking Industry Committee for the Girocard service and the stored-value card "GeldKarte".
- Austrian's EMV offline PIN solution

The European Committee for Standardization (CEN, French: Comité Européen de Normalisation) publishes the standard for accessing peripherals on EFTPOS terminals and ATMs -- including accessing the EPP (Encrypting PIN Pad) that supports the relevant security standards -- called XFS (extensions for financial services).

4 What Can Ergonomics Provide?

4.1 Security Consulting

Ergonomics can support you in recognizing and resolving enterprise wide IT risks, dangers, and weak spots. Over the years, Ergonomics security consultants have gained immense know-how – valuable in tackling the most challenging organizational and technical IT security issues.

On a daily basis, we deal with issues surrounding secure IT systems and networks, information security management, data protection, crisis management, social engineering, security concepts, and security audits. Our consultants have a plethora of skills covering technical and business areas, and are therefore able to support you in defining your strategy and implementing it to a future state, or being your professional coach in close collaboration with you.

4.2 Security Training

Ergonomics demonstrates the value and benefits of IT security standards to the management and the system owners. We show, which fundamental technical and organizational requirements have to be met.

4.3 Architecture of Compliant Systems

Ergonomics has a consolidated knowledge in designing systems that take account of all security aspects – from end to end, not only one system to the other.

4.4 Design and Development

Ergonomics can help in designing and developing the required functionality in different environments:

- Client applications that access peripherals via CEN/XFS, especially the EPP
- Server applications that process PIN and cardholder sensible data
- Implementing EPP functions according to CEN/XFS or proprietary requirements
- Implementing HSM security functions as required by standards or special demands of acquirers and issuers

Ergonomics has a rich expertise in developing applications in Java and C#, and low-level programming in C and C++.

4.5 Migration

As Ergonomics has a long-standing experience in developing secure software, we are also able to help you migrating from older security standards to current ones, allowing a systematic migration by designing coexistence of old and new systems.

4.6 Quality Management

Ergonomics has a long-standing experience in quality management. Its QM team does not only accompany the in-house development, but does also help customers.

4.7 PCI Consulting and Audits

Our certified security auditors/certified security assessors accompany you from analysis right up to implementation, and ensure that the requirements of the security standards can be met.

The PCI Security Standards Council has certified Ergonomics as official QSA Company and can therefore provide consulting and audits related to the PCI DSS standard.

5 Success Stories

NCR: 30 years of experience in designing and developing software for ATMs

- Applications for several Swiss banks following the (now legacy) Swiss ATM standard Bancomat
- Multi-vendor application following the new Swiss ATM standard ATMfutura
- Applications for several German banks

NCR: EPP programming

- TR-34 functionality
- Swiss BM interface
- German ZKA requirements
- Austrian EMV Offline-PIN support

PostFinance:

- Security consulting PCI
- EMV-CAP, standard reader DP835 based on an existing PCR model with customization for PostFinance
- Security concept for exchanging secure messages between ATM and acquiring host

ep2 Technical Working Group / SIX:

- ep2 Terminal Test System

Ergonomics:

- ep2 Library for Java
- Authentication Server (EAS)
- Pre-Personalization for PKI Tokens and Cards (PrivacyPUK)

6 Conclusion

The security technologies for card-based transactions follow comprehensive standards, which require a broad understanding by the implementers.

Ergonomics is your partner in any phase of a project, starting with initial consulting over architecture and design up to final implementations accompanied by on-going quality management.

Contact: Simon Zeller, szeller@ergonomics.ch, +41 58 311 1035