FORWARD THINKING IT SOLUTIONS

WHITE PAPER

Secure Key Management in Financial Services

V1.1

1 Abstract

We constantly strive to protect our values and possessions against theft, misusage and espionage. Cryptographic technologies play an essential role in protecting us against evil adversaries by establishing secure communication between trusted parties. This is especially prevalent in payment card business, e-commerce and financial industries. As technology (both friendly end evil) are constantly evolving, you not only need regular updates to the newest technologies, but often additionally a boost in knowledge and understanding.

Many people might have heard of acronyms such as HTTPS, SSL or RSA, as they are used in modern web applications. The requirements of the financial industry as well as the techniques to fulfil these requirements are related and often similar to the technologies. However, for a stringent implementation of security, a more complete view of security requirements and cryptographic tools needs to be considered. Examples are:

- Key exchange: How to establish trust between you and your communication partner
- Key usage: How to restrict key usage to limit damage in the case of a compromised key
- Management of keys in terms of generation, storage, loading, transport, use and destruction
- Life time management of keys in terms of periodic renewal, limitation of repeated usage
- Impact and recovery in the event of a compromised key
- Implementation with the help of secure cryptographic devices such as High Security Modules (HSM), Encrypting PIN Pads (EPP), Secure Elements on Smart Cards
- Evaluation of implemented security concepts against crypto-analytic attacks such as known-plain/cipher-text, chosen-plain/cipher-text, gardening, replay, man-in-the-middle and side-channel attacks

2 Standards and Techniques

In most industries where security and protection of secrets plays an eminent roles, a standardization organisation define minimum requirements on security standards, define typical implementation technologies and perform audits to ensure the fulfilment of these standards.

The payment card industries (PCI) Security Standards Council defines standard to keep payment systems secure, so customers can trust these systems with their sensitive payment card information. It defines common practices and standards for devices and applications handling payment card transactions. The most relevant standards in this context are the Data Security Standard and PIN Security Requirements.

The Accredited Standards Committee X9 Financial Industry Standards (ASC X9) defines a set of standards for fetial financial services on how to implement symmetric and asymmetric key techniques. Additional so-called Technical Reports detail out further details, for example:

Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00

- ANSI-X9.24: How to use symmetric keys in retail financial services
- TR-31: How to securely exchange keys including their usage (so-called key block) in an interoperable manner
- TR-34: How to secure distribute symmetric keys using asymmetric techniques in an interoperable manner.

With ANSI-X9.24, TR-31 and TR-34 standards, industry-wide and generally accepted standards have emerged to cover the common security requirements. These standards are especially recognized by the PCI-DSS and PCI-PIN standards. By complying with these standards, you can significantly lower total cost of ownership by relying on well-tested technologies that are recognized among auditors.

2.1 ANSI-X9.24

The ANSI X9.24-2 standard "Retail Financial Services Symmetric Key Management" consists of three parts:

- Part 1: Using Symmetric Techniques
- Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
- Part 3: Derived Unique Key Per Transaction

2.2 TR-31

TR-31 is a companion to the ANSI X9.24-1 standard, which defines an interoperable format to exchange keys and other secrets. These involve:

- Definition of a common header which contains attribute information about the key
- Encrypted block that contains confidential data being exchanged/stored
- A MAC that binds the header and encrypted block

2.3 TR-34

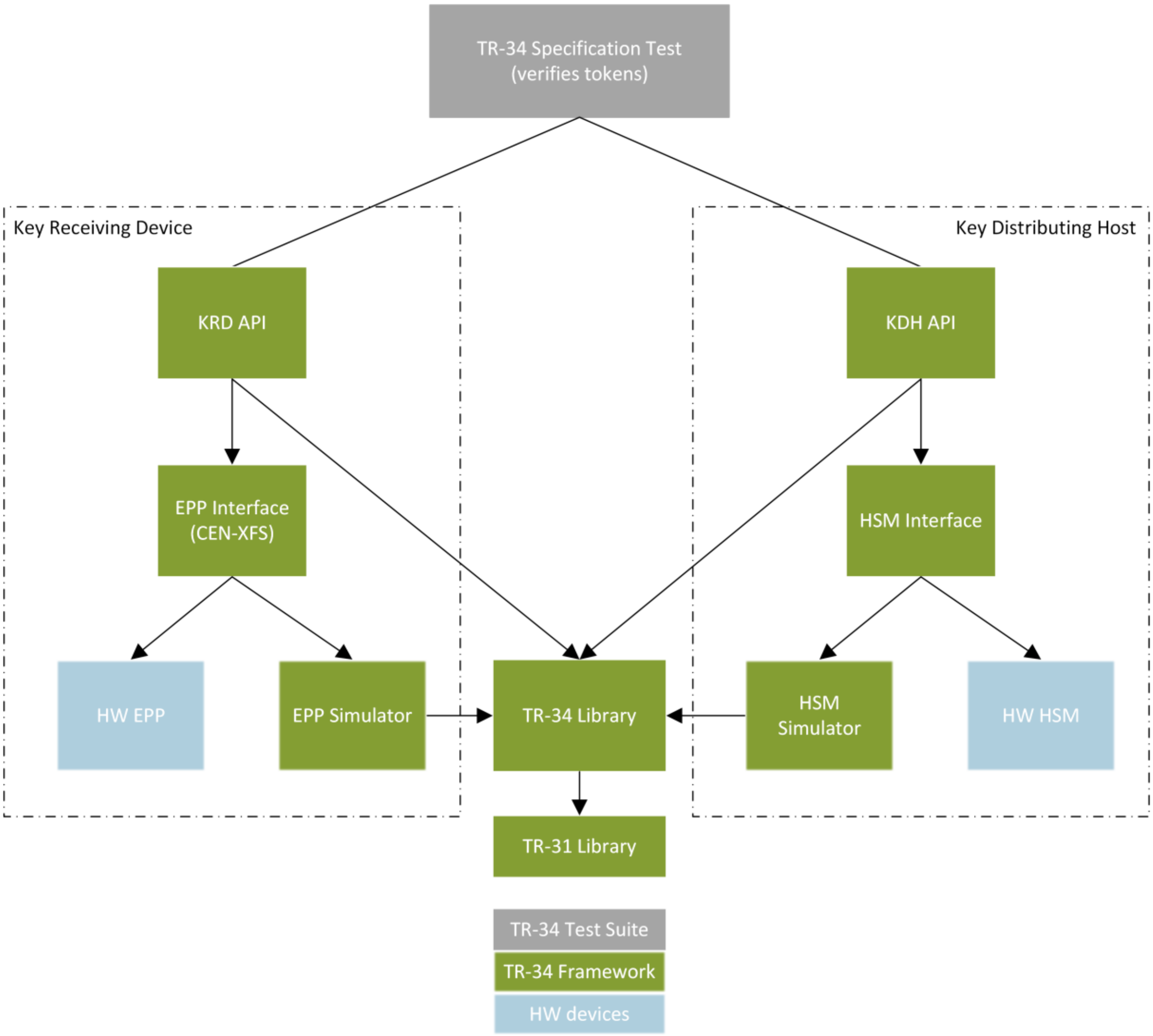
TR-34 is a companion to the ANSI X9.24-2 standard, which defines the requirements and processes for key management using asymmetric key techniques. These involve:

- Issuing public/private key certificates for both endpoints involved. These for example can be a vendor of an Encrypting PIN Pad (EPP) and the host application of an acquirer.
- Binding a pair of two endpoints together by secured exchange of a unique master key to the pair of endpoints
- Negotiating a set of transport and/or session keys based on the unique secured master key for daily communication purposes.
- Renewing expired transport and session keys
- Unbinding the secured communication channel in a secured and controlled manner and thereby terminating the secured communication channel

Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00

3 Ergonomics TR-34 Framework

The Ergonomics TR-34 Framework provides APIs and test suites for both parties in TR-34 key exchange, the Key Receiving Device (KRD) and the Key Distribution Host (KDH).



The KRD API is the Application Programming Interface of the Key Receiving Device (KRD, the terminal or the ATM) and uses either the included EPP simulator or a HW EPP.

The KDH API is the Application Programming Interface of the Key Distributing Host (KDH) and uses either the included HSM simulator or a hardware HSM.

The TR-34 Library parses and generates the TR-34 tokens. The TR-31 Library provides support for the interpretation and generation of the TR-31 key blocks, especially the Key Block Header (KBH) used in the TR-34 specification in the Symmetric Key Transport phase.

Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00

All the components may write (configurable) exhaustive log entries when parsing and creating the tokens including intermediate results, which facilitates the detection of implementation errors.

The Ergonomics TR-34 Framework is currently available as a Java library. It is also available as a C# or C++ library on request.

The library supports the following phases of the ANSI X9 TR-34 specification:

- 7.5 KDH Bind Phase
- 7.6 Symmetric Key Transport Phase
- 7.8 Symmetric Key Verification Phase
- 7.9 KDH Unbind Phase
- 7.10 KDH Rebind Phase

3.1 Use Cases

3.1.1 Manufacturer of Terminal Software

On the one hand, the KRD API of the Ergonomics TR-34 Framework enables the manufacturer of terminal software to verify the TR-34 tokens supplied by the host and helps in troubleshooting if the HW EPP does not accept these tokens.

On the other hand, using the KDH API of the TR-34 Framework, he can easily create a host simulator to test TR-34 relevant operations in the terminal software.

3.1.2 Manufacturer of Host Software

The manufacturer of host software can either integrate the Ergonomics TR-34 Framework into his host software and address his HW-HSM via the KDH API using the HSM interface or verify his own implementation of the TR-34 phases using the KDH API.

The KRD API helps on the one hand to verify the tokens supplied by the terminal and on the other hand to implement a terminal simulator for testing the host implementation.

Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00

3.2 KRD API (Key Receiving Device)

3.2.1 Bind

Retrieves the KRD credential and stores the KDH credential, according the specification steps:

- 7.5.2 Prepare KRD Credential Token (A1)
- 7.5.5 Validate KDH Credential (A2)

3.2.2 Key Transport

Generates the random number, verifies the transport token and stores the Key Block Protection Key (KBPK), according to the specification steps:

- 7.6.2 Generate Random Number Token (A1)
- 7.6.9 Verify Key Token (A2)

3.2.3 Key Transport Verification

Generates the Key Check Value (KCV), according to the specification step:

- 7.8.2 Generate Key Check Value (A1)

3.2.4 Unbind

Generates the random number and verifies the unbind token, according to the specification steps:

- 7.9.2 Generate Random Number Token (A1)
- 7.9.5 Verify Unbind Token (A2)

3.2.5 Rebind

Generates the random number, verifies the rebind token and stores the new KDH credential, according to the specification steps:

- 7.10.2 Generate Random Number Token (A1)
- 7.10.5 Verify Rebind Token (A2)

Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00

3.3 KDH API (Key Distribution host)

3.3.1 Bind

Parses the KRD credential and returns the KDH certificate, according to the specification steps:

- 7.5.3 Validate KRD Credential Token (B1)
- 7.5.4 Prepare KDH Credential Token (B2)

3.3.2 Key Transport

Parses the KRD random number and returns the key transport token, according to the specification steps:

- 7.6.3 Receive Random Number Token (B1)
- 7.6.4 Generate transported TDEA Symmetric Key (B2)
- 7.6.5 Generate Ephemeral Symmetric Key (B3)
- 7.6.6 Encipher Key Block (B4)
- 7.6.7 Encipher Ephemeral Key (B5)
- 7.6.8 Construct Key Token (B6)

3.3.3 Key Transport Verification

Parses and checks the KRD Key Check Value (KCV), according to the specification step:

- 7.8.3 Verify Key Check Value (B1)

3.3.4 Unbind

Parses the KRD authentication data and returns the unbind token, according to the specification steps:

- 7.9.3 Receive Random Number Token (B1)
- 7.9.4 Generate Unbind Token (B2)

3.3.5 Rebind

Parses the KRD random number and returns the rebind token, according to the specification steps:

- 7.10.3 Receive Random Number Token (B1)
- 7.10.4 Generate Rebind Token (B2)

»ergonomics
Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00

4 What can Ergonomics provide?

Ergonomics supports your TR-34 projects in a number of ways:

Consulting

- Knowledge about TR-34 mechanisms
- Knowledge about key management, key life cycle
- Knowledge about EPPs (CEN/XFS)
- Analysis of your key distribution and management processes against cryptographic attack scenarios
- Assisting you in the creation of secure key management concepts
- Experience in transition from legacy mechanisms to TR-34 mechanisms following PCI security standards

Engineering

- implementing TR-34
- specifying secure messaging between client (KRD) and host (KDH)

Test-Tools

- produces test-input in form of TR-34 tokens (Bind, Unbind, Rebind, Key Transport)
- validates output for TR-34 mechanisms for HSMs and EPPs
- tests overall flow of TR-34 mechanisms
- using simulates Endpoints EPP and/or HSM or real hardware

Software libraries

- producing, parsing and validating TR-34 tokens (TR-34 key blocks)
- producing, parsing and validating TR-31 key blocks, including the variant Thales key block

Hardware Knowledge

- EPP (CEN/XFS)
- HSM (Thales)

4.1 Glossary

ASC X9	ANSI (American National Standards Institute) accredited standards developing organization, responsible for developing voluntary open consensus standards for the financial services industry in the U.S.
EPP	Encrypting PIN pad
HSM	High Security Module
CEN	Comité Européen de Normalisation
XFS	eXtensions for Financial Systems
KRD	Key Receiving Device
KDH	Key Distribution host
PCI	Payment Card Industry

Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00

5 Success Stories

Consulting for new PCI compliant mechanisms for both host-to-terminal and host-to-host key exchange. The solution for host-to-terminal is based on ANSI X9 TR-34 and TR-31 standards, the solution for host-host is based on the traditional key exchange by key custodians for the exchange of the Zone Master key followed by key exchanges based on TR-31 key blocks. Additionally, Ergonomics assists the implementer of the PostFinance ATM software (SBS) in building a host simulator software that supports TR-34 by providing the KDH API of the Ergonomics TR-34 framework written in Java.

Design and implementation of a TR-34 test tool used by NCR to be an aid for Engineering and Support staff to assist external customers in their developments towards successfully implementing the TR-34 protocol. This Windows application written in C# analyzes all NCR supported TR-34 tokens, verifies imported tokens against expected values and visually displays and differences and is able to recalculate message digests and signatures.

6 Conclusions

Progress in both good and evil technology outdate and obsolete many traditional key management processes. Being not fit to the task anymore. Standardization organizations require technology and concept updates to reliably ensure minimal security standards among their partners. Transitioning from legacy and proprietary key exchange mechanisms to well-accepted industry standards such as ANSI X9 TR-34 and TR-31 greatly improves your security standards, but severely affects the security design of your IT projects. If the implications are not well considered, a poorly chosen key exchange solution might increase system complexity, costs, missed project goals and results in increased frustration.

Ergonomics is your partner in any phase of your TR-34 projects, 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

Ergonomics AG » Nordstrasse 15 » CH-8006 Zürich
info@ergonomics.ch » www.ergonomics.ch
+41 58 311 10 00