CryptoServer 2000

Summary of the Security study of CryptoServer 2000 hardware and firmware (V1 version) from Utimaco Safeware AG for implementation as SecurityBox in electronic cash networks

Translation of the Evaluation Report Summary
written by T-Systems ISS GmbH, 2003-03-11

Translation: **2003 by Utimaco Safeware AG**
Office Aachen
Germanusstrasse 27
D-52080 Aachen

Phone: ++49 241-1696-240

Telefax: ++49 241-1696-222

Internet: www.utimaco.com

E-Mail: info.de@utimaco.de

Document-Number:

Document-Version:

Date: 5th June 2003

Author:

Table of Contents

1 Introduction

Utimaco's hardware security module **CryptoServer 2000** was approved by ZKA (*Zentraler Kreditausschuss*, the umbrella association of the German credit services sector) in december 2002 for the implementation in electronic cash networks (see [ZKAApproval]). This approval was based on the (german) evaluation report

> Security study of CryptoServer 2000 hardware and firmware (V1 version) from Utimaco Safeware AG for implementation as SecurityBox in electronic cash networks

written by T-Systems ISS GmbH, 04.12.2002 (see [4]).
Since this security study is confidential, T-Systems has abstracted the non-confidential parts of the study in the following (german) document

> Summary of the Security study of CryptoServer 2000 hardware and firmware (V1 version) from Utimaco Safeware AG for implementation as SecurityBox in electronic cash networks

written by T-Systems GEI GmbH, 11.03.2003 (see [EvalReportSummary]).

The present document is the translation of parts of this summary report. The original summary report contains the chapters

1. Introduction
2. Summary of results
3. Glossary
4. Reference documents

Annexe: Evaluation and construction criteria for electronic cash systems

In this document only the capters 1, 2 and the Annexe are translated. The glossary and the reference documents can be found in the german original text [EvalReportSummary].

2 Translation of the Summary

2.1 Introduction

The CryptoServer 2000 from the Utimaco Safeware AG company is aimed at being implemented as a security box (herein after called SBox) in different electronic cash networks (POS, POZ) of the German credit services sector. These networks are connected with the authorisation centres (AS) and personalisation centres (PS) of the German credit services sector for online authorisation.

As an admission requirement for the processing of EC-cards in these networks, the German credit services sector calls for expert's report stating the compliance with the security requirements stipulated in [3].

The security components of the SBox are exclusively placed in a special-protected component, the CryptoServer. The T-Systems GEI GmbH BU ITC Security, the former T-Systems ISS GmbH, has been commissioned to analyse the security characteristics of the CryptoServer 2000 for use in the electronic cash networks of the German credit services sector.

The study analyses the available security hardware and software mechanisms of the CryptoServer, whereas a specific application – e.g. for a network provider – is not the subject of this study.

Appraisal of results is to be found in the following report:

> Security study of CryptoServer 2000 hardware and firmware (V1 version) from Utimaco Safeware AG for implementation as SecurityBox in electronic cash networks, T-Systems ISS GmbH, 04.12.2002 [4]

Results were presented to ZKA and led to a positive appraisal of CryptoServer 2000 with respect to its implementation in the German credit services sector.

The complete report includes:

- in section 2: a **summary of study results**
- in section 3: a full description of the **analysis of the SBox hardware**
- in section 4: the **SPA/DPA test** and
- in section 5: the **analysis of firmware**

This report includes:

- in section 2: merely **the summary of study results**

The annexe of this report contains the security criteria [2] of the German credit services sector which are the basis for the appraisal of results.

For the verification of the compliance with protective measures for the CryptoServer hardware and firmware, its warranted characteristics have been analysed and evaluated using the security criteria of the German credit services sector.

The complete report is divided into two sections:

Section 1: Hardware analysis

Here safety precautions of the CryptoServer hardware have been analysed with regard to the compliance with the following criteria

II	Integrity of messages
IV	Secrecy of PINs and cryptographic keys
VII	Hardware requirements
IX	Process security

Section 2: Firmware analysis

Here safety precautions of the CryptoServer firmware have been analysed with regard to the compliance with the following criteria

II	Integrity of messages
IV	Secrecy of PINs and cryptographic keys
VI	Key management
IX	Process security
XI	Encryption procedures and
XII	Non-ambiguous representation

2.2 Summary of results

The security study dealing with the CryptoServer 2000 hardware and firmware has stated that **its implementation in electronic cash networks fulfils the security requirements of the German credit services sector**.

Subject of the analysis are the sensor technology and structural shape of the SBox, its behaviour against side channels attacks (SPA/DPA), as well as its firmware providing the basic functionality for the SBox operation.

The positive evaluation is based on the following results:

The affirmation takes into consideration the attacker's state of knowledge of the hardware construction details. It also differentiates between the attack targets that an attacker can achieve.

Depending on the level of awareness it is important to distinguish between:

- **Outsiders** and
- **Insiders**

Outsiders have no information about the device construction, but they are partly able to get information about its type of construction by analysing a similar device. Insiders know about the device construction, but not about the cryptographic keys being used.

Attack targets:

1. Logging and decrypting of **customer's PIN**
2. Readout of **cryptographic keys**

The overall impact of the protective mechanisms implemented has been evaluated as follows:

1. **Any outsider's attempt to read out PINs or keys by manipulation or to defraud customers through falsified procedures fails with the utmost probability.**

2. **Any insider attempt to get keys relevant to the ec systems, also by destroying the SBox, fails with certainty as these keys are being reliably deleted.**

3. **Manipulation attempts of the SBox coming from insiders and aiming at spying out the customer's PINs would require high technological costs but they are little promising. Moreover, they leave external marks on the SBox which can be detected during a competent inspection.**

4. **A successful attack coming from outsiders or insiders using SPA/DPA analysis or combined SPA/DPA would be very doubtful, even if based on insiders' information.**

5. **Firmware complies with the security requirements for storing and processing of sensitive information in electronic cash networks.**

Overall evaluation:

In respect of the applicable criteria of the German credit services sector, the following individual assessment results from the security analysis of hardware and firmware:

ad II Integrity of messages

The type of construction of the CryptoServer in conjunction with the sensor technology ensures that stored information could not be manipulated without that being detected and defended by the sensor technology and leading to the decommissioning of the CryptoServer in electronic cash networks.

ad IV Secrecy of PINs and cryptographic keys

The hardware analysis stated that PINs and cryptographic keys can be stored only in system components which are by sensor technology effectively protected against the attempt of unauthorised readout.

ad VI Key management

CryptoServer 2000 provides the opportunity to store cryptographic keys within an available databank. Herein, keys are encrypted with CryptoServer specific $K_{CS2.}$

ad VII Hardware requirements

The requirement about storage of security-relevant information on media protected against unauthorised readout is ensured by the CryptoServer's type of construction and the sensor technology. No security-relevant information can be read out by attacks which accept the destruction of the hardware.

ad IX Process Security

The CryptoServer's type of construction and the sensor technology ensure the fulfilment of the requirements for process security.

ad XI Encryption procedures

CryptoServer 2000 provides the Triple-DES and RSA encryption procedures which, if keys of adequate length are used, meet today's technology standards.

ad XII Non-ambiguous representation

Each CryptoServer possesses an individually generated 24 bytes Triple-DES key, as well as a uniquely assigned device identifier.

2.3 Annexe – Evaluation and construction criteria for electronic cash systems

Preliminary remarks

The electronic cash system of the German credit services sector is based on a PIN-based authorisation within the authorisation systems of the German credit services system or within the chip of the chip card. Additionally, the verification of the MM character can be optionally implemented in order to guarantee the authenticity of magnetic-stripes cards.

Security-relevant data generated or provided by credit services locations are imported into the terminal HSMs (*notice of translator: hardware security modules*) of the electronic cash system via online personalisation (OPT, comp. [OPT] and [OPTDAT]) carried out by the personalisation centres of the German credit services systems.

An electronic cash network operator can administrate the sensitive functions such as “online registration” (comp. [OPTREG]) and / or “online pre-initialisation” (comp. [OPTVOR]) within the framework of online personalisation of the terminal HSMs.

In view of the applicable payment guarantee provided by the German credit services sector for its payment system “electronic cash”, the components and subsystems of this payment system must comply with the security requirements of the German credit services sector.

Security requirements are implemented based on system characteristics, type of system software and hardware and network operation. The compliance with the security requirements has to be demonstrated over all detailed stages of the electronic cash system architecture. Therefore, the consistency of consecutive specification layers, ranging from the system and interface specifications of the German credit services sector to the hardware and software implementation, has to be evaluated for all security functions, including the online registration and online sign-out, as well as the online pre-initialisation and online announcement of decommissioning. This requires an explicit description of a security model for the concerned electronic cash network which is compatible with the security requirements. This model must identify the components involved, as well as the internal and external network communication relationships.

The following criteria have to be met in order to comply with the security requirements:

I Component authentication

All components actively participating in the communication process within the electronic cash system have to authenticate one another via cryptographic procedures.

Explanation:

a) Acceptable cryptographic procedures are constricted by requirement XI.

b) Through this requirement no specific authentication procedure is settled. Generally, component authentication takes place via the proof of the possession of some secret information.

c) A component is actively participating in the communication process if it is able to evaluate, change or edit security-relevant information from its position within the system. Such information is especially the personal identification number (PIN), PIN faulty operation counter, Message Authentication Codes (MACs), transaction and disposal amount and, where applicable, the MM character. Examples of such components are:
   - The chip card
   - PIN pads
   - Security modules for carrying out re-encryption and MAC-generating procedures.
   - Security boxes for re-encrypting PINs or MACs.
   - Modules participating in the verification of MM characters.
   - Authorisation systems

d) Authentication between the chip card and the external world includes the verification of the chip card authenticity.

II Message integrity

1. All security-relevant information contained in the messages has to be protected within the system components, before and after the transmission, against unauthorised change by appropriate means.
2. Changes of security-relevant information during transmission between system components have to be detected. Corresponding reactions on integrity violation must take place.
3. Unauthorised import of messages must be detected. Corresponding reactions must also take place in case of re-imported messages.

Explanation:

a) Security-relevant information are especially identification and authentication attributes, sequence counters or transaction and disposal amounts.

b) For the requirement 1. please consider criterion VII.

III User authentication

Each user authenticates himself towards an electronic cash system by using his PIN. It must be ensured that only the knowledge of the right identification number enables one to use a chip card or carry out a specific function.

If within a component of the electronic cash system there is the additional possibility to carry out MM verifications, the authenticity of the chip cards within the MM-secured terminals must be verified at each payment transaction by means of the MM character. If and only if this MM verification should give a positive result and the PIN has been correctly entered, a further procedure will be accepted as ec transaction.

Explanation:

a) For the use of a chipcard, the user must authenticate against his chip card by entering the correct PIN.
b) Please consider the requirements 1. and 2. from the criterion IV.
c) If a terminal is designed for the MM verification but this verification is not possible due to a failure, no electronic cash payment transactions are allowed at this specific terminal.

IV Secrecy of PINs and cryptographic keys

1. A PIN must never be transmitted in clear text outside of secured sectors. In the event that it will be edited or stored in the system components, the PIN must be protected against unauthorised readout or change.
2. Cryptographic keys must in electronic communication lines never be transmitted in clear text. In the event that they will be used or stored in the system components, they must be protected against unauthorised readout and change.
3. No system component must give the opportunity to identify a PIN due to exhaustive search.

Explanation:

a) Requirement 1. is to keep since the PIN entering over the keyboard.

   PIN transmission in clear text from the keyboard to the user's chip card is acceptable only if it is ensured that the entered PIN code does never leave the physically secured sector including the contacts of the chip card and that it cannot be recorded within this sector.
b) Please consider criterion VII for the hardware components (e.g. PIN pads and chip cards) in which PINs or keys are to be stored or processed.
c) Cryptographic keys are particularly those used for the PIN encryption, MAC generation, MM verification and MM transmission.

V Logging

1. In the electronic cash system all data required for the reconstruction of related processes must be logged.
2. Evaluation of log information must take place in a regulated manner.
3. Saved log data must be protected against unauthorised change and able to be forwarded to an evaluating body.

Explanation:

a) E.g. the following cases of security violations and irregularities in electronic cash networks are to be logged:
   - faulty transmission
   - multiple initialisation of individual components
   - no electronic cash transaction over a longer period
   - multiple invalid PIN entrance

- negative MM verification result
- re-imported messages

b) Criterion XIII is to be considered.

VI Key management

1. Arrangements are to be made for distribution, administration and possibly rotational change and replacement of keys, particularly with regard to key exchange in cases of compromise.
2. Keys suspected of being compromised are not allowed anymore to be used in the entire electronic cash system.
3. For symmetric encryption procedures, dynamic procedures for MAC generation and encryption, particularly PIN encryption, between all components of the electronic cash systems must be used.
4. For different security functions, such as PIN encryption, MAC generation and, if necessary, MM transmission, different keys must be used.
5. All keys used in the electronic cash system must be protected against unauthorised access and stored in security modules. Keys could also be stored outside of security modules if having been encrypted with a key which is stored in the security module and if it is impossible to re-import keys which should no longer be used.

Explanation:

Criterion XIII should be considered.

VII Hardware requirements

1. All encryption, decryption, and re-encryption procedures, MAC generation, as well as cryptographic verification procedures and, if necessary, the MM verification are carried out in components (security modules) which are highly protected against unauthorised access. Corresponding keys are also stored in such security modules.
2. In security modules, security-relevant data and procedures (e.g. keys, programs) must be protected against unauthorised change and secret data (e.g. keys, PINs) must be protected against unauthorised readout. You should provide for these aspects by taking the following measures:
   - type of construction of the security module, possibly in conjunction with the security mechanisms of the security module software.
   - program loading into the security module only during production or cryptographic securing of the loading procedure,
   - cryptographic securing of the loading procedure for security-relevant data, particularly for cryptographic keys.

   Within a security module, secret data have to be protected against the readout by means of attacks which accept the destruction of the module.

Explanation:

a) Protecting data and programs against change and readout respectively, within security modules must be a top priority so that, during the life time of the module, attacks with

reasonable expenses are made impossible, whereat the costs for a successful attack are always to weighed up against the expected profit.

b) Mechanical and electronic memory protection must be provided for in order to secure data and procedures.

c) A PIN keyboard must be protected against the adding of new construction groups.

d) The display of a security module must be protected against falsification

e) Unwanted functions must not be executable.

f) Chip cards must fulfil the requirements of this criterion. In particular chip hardware and software must ensure that the chip card is able to communicate only via the specified interface in the manner expressly specified.

VIII Organisational measures for the production and personalization of security modules

1. The production and personalisation (first insertion of secret keys, user-specific data, if needed) of security modules (particularly chip cards) must take place in a production area preventing that:
   - keys are getting compromised during the personalisation
   - the procedure of personalisation is run by an unauthorised body or in an abusive manner
   - unauthorised software and data can be inserted
   - security modules are being abstracted
2. It must be ensured that no unauthorised components performing sensitive functions could be inserted into the electronic cash systems.
3. The life cycle of all security components must be continually logged.

Explanation:

1. For the requirement 2. please consider criterion XIII
2. The logging of the life cycle of a security module must include:
   - production and personalisation data
   - regional/temporal distribution
   - maintenance and repair
   - decommissioning
   - loss or theft.

   for chip cards:
   - production and personalisation data
   - import of new applications
   - change of applications
   - change of keys
   - decommissioning
   - loss or theft.

IX Process security

It must be ensured that the processing of specified transactions and the thereby used security-relevant data of the electronic cash system could not be manipulated.

The instances involved, particularly the user, may not be deceived by the security module into the processed transactions.

Explanation:

Criterion VII is to be considered.

X Processing of other applications

The parallel processing of other applications in the components of the electronic cash system must not have any influence on the security of the electronic cash system.

Explanation:

a) It must be ruled out for instance that functions which perform the PIN processing of credit cards in the PIN pads could be abused leading to PINs being compromised in the electronic cash system.
b) If different functions can be performed within a chip card, in this case no function should have any influence on the security of another one.

XI Encryption procedures

Only encryption procedures which are able to withstand a cryptoanalysis with selected clear text must be used.

Explanation:

Security must not depend on the secrecy of procedures, it must be ensured by the secrecy of keys.

XII Non-ambiguous representation

Each security component of the electronic cash system must be clearly identifiable in the system.

Explanation:

Identification data should be used in order to assign security-relevant messages uniquely to the respective sender or recipient.

XIII Personnel requirements

1. Trustworthy persons are to be appointed to be in charge with the verification of logging data.
2. Trustworthy persons are to be appointed to be in charge with the key generation and import into security modules according to criterion VI.
3. Trustworthy persons are to be nominated for being responsible in case of changes of approved system components for security-relevant characteristics of the components either to remain unchanged or, if changed, that changes will be notified to the German credit services sector.
4. Trustworthy persons are to be nominated for being responsible for the import of software and security-relevant data into security modules.

For requirements 1 - 4 the 2-persons' rule must be considered.

3 References

	Title / Company
[EvalReportSummary]	Zusammenfassung der Sicherheitsuntersuchung der Hardware und Firmware des CryptoServers 2000 (Version V1) der Utimaco Safeware AG zum Einsatz als SecurityBox in electronic cash-Netzen / Bonn, 11.03.2003; T-Systems GEI GmbH
[ZKAApproval]	letter from ZKA to Utimaco Safeware AG (Andreas Philipp) / Berlin 18.12.2002, ZKA (Zentraler Kreditausschuss)
[2]	Technischer Anhang zum Vertrag über die Zulassung als Netzbetreiber im electronic-cash-Systemen der deutschen Kreditwirtschaft / Version 5.3.1, 5.9.2002, ZKA
[3]	Kriterien für alle Bewertungen und Konstruktionen von electronic cash Systemen / Version 5.3.1, 5.9.2002, ZKA
[4]	Sicherheitsuntersuchung der Hardware und Firmware des CryptoServers 2000 (Version V1) der Utimaco Safeware AG zum Einsatz als SecurityBox in electronic cash-Netzen / Bonn, 04.12.2002; T-Systems ISS GmbH
[OPT]	Schnittstellenspezifikation für die ec-Karte mit Chip: Online-Personalisierung von Terminal-HSMs / Version 3.0, 2.4.1998, ZKA
[OPTDAT]	Schnittstellenspezifikation für die ec-Karte mit Chip: Personalisierungsinhalte für die Online-ZKA-Personalisierung / Version 1.0, 29.12.1998, ZKA
[OPTREG]	Schnittstellenspezifikation für die ZKA-Chipkarte: Online-Registrierung und Online-Abmeldung von Terminal-HSMs / Version 1.0, 4.8.2000, ZKA
[OPTVOR]	Schnittstellenspezifikation für die ec-Karte mit Chip: Online-Vor-Initialisierung und Online-Anzeige einer Außerbetriebnahme von Terminal-HSMs / Version 1.0, 4.8.2000, ZKA