CryptoServer 2000
Security Policy

Document Version 1.1.4
Document No. 2004-0007

Utimaco Safeware AG

9th May 2005

TABLE OF CONTENTS

1. Module Overview

The CryptoServer 2000 is an encapsulated, protected security module which is realized as multi-chip embedded cryptographic module in the sense of FIPS 140-2 (Hardware Version 1.0.2.0, Firmware Version 1.0.0.2). Its realization meets FIPS 140-2 overall level 3 requirements, with level 4 requirements in section “Physical Security”. The primary purpose for this module is to provide secure cryptographic services like en- or decryption (for various cryptographic algorithms like Triple-DES, RSA and AES), hashing, signing and verification of data, random number generation, on-board secure key generation, key storage and further key management functions in a tamper-protected environment.

In FIPS mode, the module offers a general purpose API with FIPS Approved algorithms for the above mentioned cryptographic services, as well as an administrative interface. A Secure Messaging concept protects the communication to and from the module by message encryption and MAC authentication.

If not in FIPS mode, the CryptoServer’s flexible software architecture allows its usage in nearly all proprietary environments where cryptographic services and highest security are required: for instance in archiving systems and payment systems, it can serve as a signature server, time stamp and as a generator for PINs, cryptographic keys or random numbers. In non-FIPS mode, the CryptoServer offers hardware based as well as deterministic random number generation.

The CryptoServer 2000 is encased in a hard opaque commercial grade metal case which contains a tamper response envelope around the module: All hardware components of the cryptographic module (including the Central Processing Unit, all memory chips, Real Time Clock and hardware noise generator for random number generation) are located on a printed circuit board and encapsulated by metal shells, a special tamper detection envelope (which is a special foil bearing a flexible printed circuit with a serpentine geometric pattern of conductors) and potting material. This hard, opaque enclosure defines the cryptographic boundary of the module as is illustrated in the picture below.

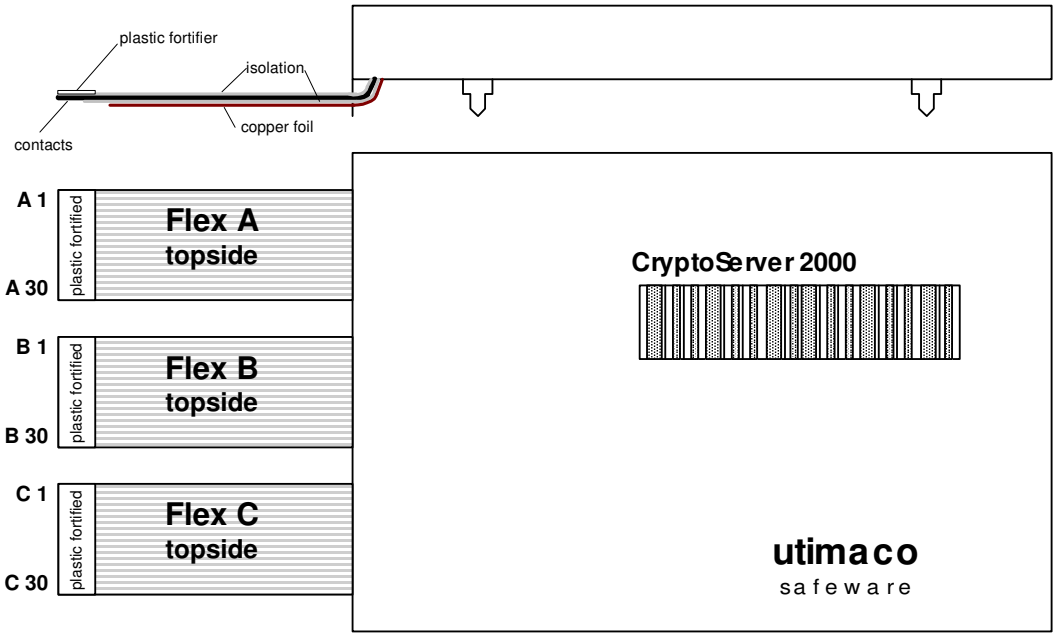

Figure 1 – CryptoServer 2000 (cryptographic boundary)

To enable communication with a host, this encapsulated cryptographic module is mounted on a carrier card which supports a PCI interface and two serial interfaces (RS232). The connection between the cryptographic module and the carrier card is done by the three ribbon cables shown in figure 1. The following picture shows the cryptographic module CryptoServer 2000 mounted on a PCI carrier card:

Figure 2 – CryptoServer 2000 mounted on the PCI carrier card

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2. In the section "Physical Security" level 4 is reached.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

3. Modes of Operation

Approved mode of operation

In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- RSA with variable key sizes (minimum 1024 bit key length) for
  - Sign/Verify
  - Key Wrapping/Unwrapping (i. e. Key Encryption/Decryption)

  (see RSA Validation Certificates No. 25 and 49)
- Triple-DES (TDES) for
  - Data Encryption/Decryption
  - Key Wrapping/Unwrapping (i. e. Key Encryption/Decryption)

  (see Triple DES Modes of Operation Validation Certificate No. 284)

- AES for
    - Data Encryption/Decryption
    - Key Wrapping/Unwrapping (i. e. Key Encryption/Decryption)

  (see Advanced Encryption Standard Validation Certificate No. 182)
- SHA-1, SHA-224 and SHA-256 for hashing
  (see Secure Hash Standard Validation Certificates No. 268 and 297)
- TDES-MAC
  (vendor affirmed, based on FIPS Approved Triple-DES core algorithm, see Validation Certificate No. 284)

The Single-DES algorithm is not supported in FIPS-mode.

The CryptoServer 2000 supports the commercially available Diffie-Hellmann protocol *[PKCS#3]* for key establishment (see below for the *Secure Messaging* concept).

Furthermore the CryptoServer 2000 in FIPS mode offers key generation services:

- RSA key pair generation
- Triple-DES key generation
- AES key generation

For random value generation and generation of all cryptographic keys, the CryptoServer 2000 relies on an implemented deterministic random number generator (DRNG) that is compliant with ANSI X9.31, Appendix A.2.4 with 112 bit seed key and 64 bit seed (see *[ANSIX9.31]*). This DRNG is FIPS Approved, see Random Number Generator Validation Certificate No. 34.

Seed and seed key for the DRNG will be generated by the CryptoServer's non-deterministic random number generator (NDRNG) which is based on a hardware noise source.

The CryptoServer 2000 may be configured for FIPS mode by loading all FIPS certified firmware into a module that is in delivery state and performing a power cycle as described in the CryptoServer's *Administrator's Guide for CryptoServer in FIPS Mode [CS2AdmGuide]*. If this has been performed successfully, the module's internally stored *FIPS mode indicator* flag is set. The user can observe if the cryptographic module is running in FIPS vs. non-FIPS mode via execution of the "GetState" service where the FIPS mode indicator will be displayed.

Non-FIPS mode of operation

In non-FIPS mode, additional firmware can be downloaded into the cryptographic module that provides non-FIPS Approved algorithms as follows:

- IDEA
- Safer
- RSA for public key cipher of bulk data

- MD5, MDC-2 or RIPEMD-160 for hashing
- Single DES (not being validated for FIPS 140-2 standard)
- Retail-TDES MAC
- AES MAC
- Key generation with True Random Number Generator (based on a physical noise source)
- PIN generation / PIN verification (e. g. VISA / MasterCard)

Secure Messaging for secure communication with the CryptoServer

The CryptoServer 2000 implements a *Secure Messaging* concept which enables any operator to secure his communication with the CryptoServer over the PCI interface, even from a remote host. With Secure Messaging, commands sent to the CryptoServer and answer data received from the CryptoServer may be encrypted and integrity-protected/signed with a TDES MAC. In FIPS mode, Secure Messaging has to be performed for every sensitive command, i. e. for every command that is only available for authenticated users.

To do Secure Messaging, the operator has to open a (Secure Messaging) *Session*. For a Session, a 16 bytes TDES session key will be negotiated between CryptoServer and host via Diffie-Hellmann algorithm as key establishment technique (according to *[PKCS#3]*; for generation of its random value needed for the key agreement, the CryptoServer will use its deterministic random number generator).

The CryptoServer can simultaneously manage multiple Sessions (with multiple operators): Each Session manages its own session key, which is identified by a session ID. All commands using the same session ID and the same session key are said to belong to one session. In this way a secure channel will be established between the CryptoServer and the host application.

4. Ports and Interfaces

The CryptoServer 2000 is connected to the outside word using three ribbon cables: Flex A, B and C, each consisting of 30 signal lines (see figure 1). The device provides three physical ports on these ribbon cables:

1) Power input (including operational power input and backup power input).
2) An external bus which is used for data input, data output, control input and status output.
3) An External Erase input, which can be used to zeroize all secret information inside the module.

To enable communication with a host, the encapsulated cryptographic module is mounted on a carrier card which supports a PCI interface and two serial interfaces (RS232). The carrier card maps the external bus of the module to the PCI and serial interfaces. All requests for services are sent over the PCI interface. The first serial interface is used for status output only. The second serial interface is not used in FIPS mode.

The input and output of all Critical Security Parameters (CSPs) will be done over the services that are offered over the PCI interface. In particular, CSPs will be entered and output only in an encrypted form: All command and answer data (except for status requests) to and from the CryptoServer will be encrypted and MAC protected by the Secure Messaging layer, see previous subsection *Secure Messaging for secure communication with the CryptoServer*. Additionally, all secret or private keys can only be imported or exported in a wrapped form, i. e. encrypted (via the services *Import Key* and *Export Key*, see section 6 *Roles and Services).*

5. Identification and Authentication Policy

Assumption of roles

The CryptoServer cryptographic module supports two distinct operator roles: *Cryptographic User* and *Administrator* role (called *User Role* respectively *Crypto Officer Role* in [FIPS140-2]). Additionally a Public User is allowed to perform any non-sensitive services like requesting status information without prior authentication. The cryptographic module enforces the separation of roles using identity-based operator authentication. Two authentication methods are supported by the module: Password authentication and RSA signature authentication.

For *password based authentication* the operator must enter a user name and his password to log in. The user name is an alphanumeric string of up to 8 characters. The password is a binary string of 16 bytes (which may contain an alphanumeric string), a minimum of 6 bytes must be different from zero or blank.

For *RSA signature based authentication* the user sends a RSA signed command containing his user name to authenticate to the cryptographic module.

Upon correct authentication, the role is selected based on the user name of the operator. During authentication a session key is negotiated which is used to secure subsequent service requests of the operator (see the description of the Secure Messaging concept, page 8). Since the session key (and session ID) is stored in volatile memory, all information about the authentication and session is lost if the module is powered down.

The CryptoServer 2000 supports multiple simultaneous operators, each using his own session key for message authentication of the service requests. This ensures the separation of the authorized roles and services performed by each operator.

At the end of a session, the operator may log-out, or, after 15 minutes of inactivity, the session key will be invalidated inside the cryptographic module.

Table 2 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic User (called *User* in [FIPS140-2])	Identity-based operator authentication	User Name and Password or User Name and RSA Signature
Administrator (called *Crypto Officer* in [FIPS140-2])	Identity-based operator authentication	User Name and Password or User Name and RSA Signature

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password (6 characters password chosen out of 94 printable ASCII characters)	The probability that a random attempt will succeed or a false acceptance will occur is 1/689,869,781,056 which is less than 1/1,000,000. Due to a correctional delay of 40 milliseconds for every non-successful authentication (s. t. there is a maximal limit of 1500 non-successful authentications per minute), the probability of successfully authenticating to the module within one minute is (less than) 1/459,913,187 which is less than 1/100,000.
RSA Signature (1024 bit key)	The probability that a random attempt will succeed or a false acceptance will occur is approximately 2^{-1024} which is less than 1/1,000,000. Due to a correctional delay of 40 milliseconds for every non-successful authentication (s. t. there is a maximal limit of 1500 non-successful authentications per minute), the probability of successfully authenticating to the module within one minute is less than 2^{-1014} which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
Cryptographic User: This role provides all cryptographic services, i. e. services for management and usage of private, public and secret keys, hashing services and random number generation.	• Change Cryptographic User's Password or Key: This service will change the password or RSA public key which is used for the *Cryptographic User's* authentication. • Get Session Key: This service generates a new session key for secure communication to the module. • Crypt Data: This service encrypts or decrypts data using a TDES or AES key in CBC or ECB mode. • Calculate MAC: This service calculates a TDES-MAC over given data. • Sign Data: This service generates a RSA signature. • Verify Signature: This service verifies a RSA signature. • Calculate Hash: This service calculates a SHA-1, SHA-224 or SHA-256 hash value over given data. • Generate Random Number: This service generates a random number using the DRNG. • Generate DES key: This service generates a TDES key (16 or 24 bytes) using the DRNG. In FIPS mode this service will not generate Single-DES keys. • Generate AES key: This service generates an AES key using the DRNG. • Generate RSA key: This service generates a RSA key using the DRNG. • Export Key: This service outputs a wrapped key (i. e. encrypted with a Key Encryption Key). • Import Key: This service imports a wrapped key (i. e. encrypted with a Key Encryption Key) into the cryptographic module.

Role	Authorized Services
	• Export Public Key: This service outputs the public part of a RSA key. • List Keys: This service outputs a list of all keys stored inside the cryptographic module. • Delete Key: This service deletes a key from the module.
Administrator: This role provides all services necessary for firmware and user management.	• Add Operator: This service will add a *Cryptographic User* or *Administrator* to the cryptographic module. • Delete Operator: This service will delete a *Cryptographic User* or *Administrator* from the cryptographic module. • Load File: This service loads files. If a file with the same file name is currently loaded, the current file will be replaced. This command is usually used to load and replace firmware modules. If the file is a firmware module, the old file will only be replaced if the version of the new module is higher or equal to the old module version and if the RSA signature over the firmware module is verified. (Note: Loading non-FIPS-validated software or firmware onto the cryptographic module will cause the module to no longer be FIPS-validated.) • Delete File: This service is used to delete files. • Set Clock: This service allows the *Administrator* to set the internal clock on the module. • Change Administrator's Password or Key: This service will change the password or RSA public key which is used for the *Administrator*'s authentication. • Get Session Key: This service generates a new session key for secure communication to the module.

Unauthenticated Services

Furthermore, the CryptoServer 2000 supports the following unauthenticated services, i. e. services which are available to any operator:

- Show Status: (or Get State) This service provides the current status of the cryptographic module, including the FIPS mode indicator.
- Get Time: Read the current time out of the internal Real Time Clock of the

module.

- List Files: Retrieve a list of all files stored in the flash file system of the module.
- List Active Modules: List all currently active firmware modules.
- List Operators: Read a list of all *Cryptographic Users* and *Administrators*.
- End Session: Terminate a (Secure Messaging) session by invalidating the respective session key.
- Get Log File: Read a log file.
- Get Memory Info: Return statistical information regarding the file system usage.
- Echo: Communication test (echo input data).
- Get Challenge: Generate and output a challenge (8 bytes random value) for usage of the challenge/response mechanism with the next authenticated command.
- Initiate Self Tests: At any time the execution of the self-tests required by FIPS 140-2 can be forced by performing a reset or power-cycle of the module. During self-test execution no further command processing is possible.
- Zeroize: Zeroize the cryptographic module including all firmware, data and critical security parameters. This service will be executed if an external erase input is given.

If the module is in a FIPS error state, only unauthenticated services that only output status and do *not* perform any cryptographic functions are available.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Master Key (TDES 24 bytes) $\mathbf{K_{CS2}}$
- Session Key (volatile storage only)
- Seed for Deterministic Random Number Generator (DRNG) (volatile storage only)
- Seed Key for DRNG (volatile storage only).

The following CSPs are stored within the cryptographic module encrypted with the Master Key $\mathbf{K_{CS2}}$ (TDES): (Note: These non-volatile CSPs are not subject to the zeroization requirement since they are encrypted using TDES.)

- RSA Private Sign Key
- RSA Private Key Decryption Key
- TDES Key Encryption Key

- AES Key Encryption Key
- TDES Data En-/Decryption or MAC Key
- AES Data En-/Decryption Key
- *Administrator* Password (for authentication)
- *Cryptographic User* Password (for authentication)

Definition of Public Keys:

The following are the public keys contained in the module:

- Production Key (RSA 1024 bit) K_{Prod_pub}
- Module Signature Key (RSA 1024 bit) $K_{Mdl\text{-}Sig\_pub}$
- Initialization Key(RSA 1024 bit) K_{Init_pub}
- RSA Public Verify Key
- RSA Public Key Encryption Key
- *Administrator's* Public RSA Authentication Key
- *Cryptographic User's* Public RSA Authentication Key

Definition of CSPs Modes of Access

Table 5 defines the relationship between the different module services and access to CSPs. The types of access (e. g. Use/Write/Update) are given in the right column.

The following types of access are possible:

- *Write:* The CSP is created (newly written).
- *Update:* The value of the CSP will be replaced by a new value.
- *Use:* The value of the CSP is used for some cryptographic calculation.
- *Export (wrapped):* The CSP will be wrapped by some key encryption key and exported from the cryptographic module.
- *Export:* The key will be exported from the cryptographic module (only possible for public RSA keys).
- *Delete:* The CSP will be invalidated.

The two left columns indicate for which *Role* the respective service is available.

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation	Type of Access
Admini-strator	**Crypto-graphic User**			
	X	Crypt Data	*TDES or AES Data En-/Decryption Key*	Use
	X	Calculate MAC	*TDES MAC Key*	Use
	X	Sign Data	*RSA Private Sign Key*	Use
	X	Verify Signature	*RSA Public Verify Key*	Use
	X	Calculate Hash	---	---
	X	Generate Random Number	*1) Seed for DRNG*	Use and Update
			2) Seed Key for DRNG	Use
	X	Generate DES Key	*1) Seed for DRNG*	Use and Update
			2) Seed Key for DRNG	Use
			3) TDES Data En-/Decryption, MAC or Key Encryption Key	Write
	X	Generate AES Key	*1) Seed for DRNG*	Use and Update
			2) Seed Key for DRNG	Use
			3) AES Data En-/Decryption or Key Encryption Key	Write
	X	Generate RSA Key	*1) Seed for DRNG*	Use and Update
			2) Seed Key for DRNG	Use
			3) RSA Signing or Key Decryption Key	Write
	X	Export Key	*1) TDES Data En-/Decryption or MAC Key or TDES Key Encryption Key or AES Data En-/Decryption Key or AES Key Encryption Key or RSA Private Signing Key or RSA Public Verifying Key or RSA Public Key Encryption Key or RSA Private Key Decryption Key*	Export from module (wrapped, i. e. encrypted with a Key Encryption Key)

			2) TDES Key Encryption Key or AES Key Encryption Key or RSA Public Key Encryption Key	Use
			3) Seed for DRNG	Use and Update (only if wrapping is performed by RSA key)
			4) Seed Key for DRNG	Use (only if wrapping is performed by RSA key)
	X	Import Key	*1) TDES Data En-/Decryption or MAC Key or TDES Key Encryption Key AES Data En-/Decryption Key or AES Key Encryption Key or RSA Private Signing Key or RSA Public Verifying Key or RSA Public Key Encryption Key or RSA Private Key Decryption Key*	Write or Update
			2) TDES Key Encryption Key or AES Key Encryption Key or RSA Public Key Encryption Key	Use
	X	Export Public Key	*RSA Public Key Encryption Key or RSA Public Verifying Key*	Export
	X	List Keys	---	---
	X	Delete Key	*TDES Data En-/Decryption or MAC Key or TDES Key Encryption Key or AES Data En-/Decryption Key or AES Key Encryption Key or RSA Private Signing Key or RSA Public Verifying Key or RSA Public Key Encryption Key or RSA Private Key Decryption Key*	Delete
X		Load File	*1) Public Module Signature Key*	Use
			2) Public Initialization Key	Use
X		Delete File	---	---
X		Set Clock	---	---

X		Add Operator	*Public RSA Authentication Key or Password of operator*	Write
X		Delete Operator	*Public RSA Authentication Key or Password of operator*	Delete
X	X	Change Operator	*Public RSA Authentication Key or Password of operator*	Update
X	X	Get Session Key	*1) Seed for DRNG*	Use and Update
			2) Seed Key for DRNG	Use
			3) Session Key	Write
			4) Public Initialization Key or Public RSA Authentication Key or Password of operator	Use
X	X	End Session	*Session Key*	Delete
	X	any command authentication performed by *Cryptographic User*	*Public RSA Authentication Key or Password of Cryptographic User*	Use
X		any command authentication performed by *Administrator*	*Public Initialization Key or Public RSA Authentication Key or Password of Administrator*	Use
X	X	any command using *Secure Messaging*	*Session Key*	Use

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Cryptographic Module does not contain a modifiable operational environment.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the

security requirements of this FIPS 140-2 Level 3 module.

1. The cryptographic module provides two distinct operator roles. These are the *Cryptographic User* role and the *Administrator* role.
2. The cryptographic module provides identity-based authentication.
3. When the module has not been placed in a valid role, the operator has no access to any cryptographic services.
4. The cryptographic module performs the following tests:
   a) Power up Self-Tests:
      i) Cryptographic Algorithm Tests:
         (1) TDES Known Answer Test
         (2) TDES-MAC Known Answer Test
         (3) AES Known Answer Test
         (4) SHA-1, SHA-224 and SHA-256 Known Answer Tests
         (5) RSA Known Answer Test (sign/verify and encrypt/decrypt)
         (6) ANSI X9.31 DRNG Known Answer Test
      ii) Software Integrity Test (CRC (16 bit) for boot loader program code, RSA signature verification for firmware)
      iii) Critical Functions Tests
         (1) SDRAM Test
         (2) Master Key Integrity Test
   b) Conditional Self-Tests:
      i) Continuous *Random Number Generator (RNG) Test* – performed on NDRNG and DRNG
      ii) RSA Key *Pairwise Consistency Test* (sign/verify and encrypt/decrypt) for RSA key generation
      iii) Software Load Test (via RSA signature verification)
5. At any time the operator is capable of commanding the module to perform the power-up self-test.
6. Prior to each use, the ANSI X9.31 DRNG and the hardware based NDRNG is tested using the conditional test specified in FIPS 140-2 §4.9.2.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. The module does not allow the export of a RSA private key wrapped with a RSA public key

encryption key.

9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module supports concurrent operators.

This section documents the security rules imposed by the vendor:

1. The module zeroizes all plaintext CSPs within maximal 4 milliseconds after any attack or alarm (see section 9 below).
2. If the cryptographic module remains inactive in any valid role for a maximum period of 15 minutes, the module automatically logs off the operator.
3. The module offers the possibility to protect command and answer data on their way to and from the module via a *Secure Messaging* mechanism. This mechanism encrypts and integrity protects the data with TDES encrypting algorithm respectively MAC. In FIPS mode, the usage of secure messaging is mandatory.
4. The module implements a Challenge-Response mechanism to prevent the replay of older authenticated messages.
5. The module prohibits the export of plaintext cryptographic keys or other CSPs.
6. The module supports an attribute “Exportable” for every stored private or secret cryptographic key. The module allows the (wrapped) export of a key only if this attribute is set.
7. The module supports an attribute “Key Encryption Key” for every stored cryptographic key. If this attribute is set, the module allows the key to be used to wrap other keys (for export) but not to be used for data encryption or signing. If this attribute is not set, the module allows the key to be used for data encryption or signing, but not to be used to wrap other keys (for export). In FIPS mode, RSA keys cannot be used for bulk data encryption.

9. Physical Security Policy

Physical Security Mechanisms

The CryptoServer 2000 multi-chip embedded cryptographic module is encapsulated with a hard, opaque, tamper-evident potting coating. This coating consists of an inner metal housing surrounded by a special tamper-detection foil and potting material, and all this encased in an outer metal housing.

The CryptoServer module with its tamper-evident enclosure (the coating) implements the following physical security mechanisms:

- Active tamper response and zeroization circuitry.

- Module is entirely encapsulated by a security foil (tamper sensor) that detects all physical and chemical attacks.
- Temperature sensors that activate a tamper response if the module is outside the defined temperature range of –14°C to 66°C.
- Voltage sensors that monitor the power supply of the module and activate a tamper response if the power input is outside the defined range.
- Tamper response and zeroization circuitry is active while module is in standby mode (powered down).
- Zeroization is done within less than 4 milliseconds after tamper detection.
- Module stops operation if it is outside the operational temperature range of 5°C to 58°C.
- Regularly invert all bits of the clear text CSPs to avoid "burn in" of information into SRAM cells.

To ensure physical security of the cryptographic module, no extra action has to be performed. For a module in FIPS mode, the above listed physical security mechanisms function autonomously and under any circumstances.

To ensure functionality, the module must be periodically inspected for tamper evidence.

10. Mitigation of Other Attacks Policy

The module has been designed to mitigate Simple and Differential Power Analysis (SPA / DPA) and Timing Analysis.

Table 6 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism
SPA / DPA	SPA / DPA attacks are mitigated by use of hardware components assembled into a special design of the power management circuit, such that it is not feasible to monitor current consumption to determine the value of an algorithm's key. Current consumption of the module does not depend on the value of cryptographic keys.
Timing Analysis	It is not feasible to determine the value of an algorithm's keys by measuring the execution time of a cryptographic operation. TDES and AES operations are executed in fixed time. The input data to a private RSA operation is randomized by use of a blinding technique, so that the input parameters of the RSA algorithm are not known by the operator. For that reason it is not possible to calculate the bits of a private key by the amount of time required by the private RSA operation.

The CryptoServer's ability to mitigate effectively SPA/DPA attacks was successfully tested by the evaluator T-Systems in the context of the CryptoServer's ZKA (Zentraler Kreditausschuss) validation process.

11. References

	Title / Company
[CS2AdmGuide]	CryptoServer 2000 - Administrator's Guide for CryptoServer in FIPS-Mode, Doc. no 2004-0002 / Utimaco SafewareAG
[ANSIX9.31]	ANSI X9.31-1998: Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) / American Bankers Association, 1998
[FIPS140-2]	FIPS PUB 140-2, Security Requirements for Cryptographic Modules / National Institute of Standards and Technology (NIST), May 2001
[PKCS#1]	PKCS#1: RSA Encryption Standard v1.5, November 1993 / RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs
[PKCS#3]	PKCS#3: Diffie-Hellman Key Agreement Standard v1.4, 1st November 1993 / RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs

12. Definitions and Acronyms

CSP	Critical Security Parameter
DRNG	Deterministic Random Number Generator
NDRNG	Non-deterministic Random Number Generator
RNG	Random Number Generator
SPA / DPA	Simple Power Analysis / Differential Power Analysis
ZKA	*Zentraler Kreditausschuss*, the umbrella association of the German credit services sector