Zyt Cryptographic Module Security Policy

Document *Version 1.1*

Taua Biomatica

December 20, 2006

TABLE OF CONTENTS

1. MODULE OVERVIEW 3

2. SECURITY LEVEL 3

3. MODES OF OPERATION 4

4. PORTS AND INTERFACES 5

5. IDENTIFICATION AND AUTHENTICATION POLICY 5

6. ACCESS CONTROL POLICY 6

ROLES AND SERVICES 6
DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 8
DEFINITION OF CSPS MODES OF ACCESS 8

7. OPERATIONAL ENVIRONMENT 10

8. SECURITY RULES 10

9. PHYSICAL SECURITY POLICY 11

PHYSICAL SECURITY MECHANISMS 11
OPERATOR REQUIRED ACTIONS 12

10. MITIGATION OF OTHER ATTACKS POLICY 12

11. REFERENCES 13

12. DEFINITIONS AND ACRONYMS 13

1. Module Overview

The Zyt Cryptographic Module device is a multi-chip embedded cryptographic module (Hardware Version: HW P/N PM400002-9, Version 3; Firmware Version 2.0) encased in a hard, opaque, tamper evident epoxy. The Zyt is a Hardware Security Module (HSM) designed to encrypt and digitally sign documents/transactions. This security policy specifies the security rules that must be followed by the persons involved in its operations, the service provided by the module and the Critical Security Parameters (CSPs). The physically contiguous boundary is defined as the outer perimeter of the potted PCB containing all of the security relevant hardware required for secure cryptographic processing. The image below defines the physically contiguous cryptographic boundary.

Figure 1 – Image of the Cryptographic Module

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

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	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

The Zyt Cryptographic Module has two modes of operation as follows:

1. the FIPS Approved mode;
2. the non-FIPS mode.

It enters the FIPS Approved mode upon each power cycle. Then it may enter the non-FIPS mode when an operator authenticates to the module using cryptographically protected identity strings that are input to the module from a smart card external to the cryptographic boundary that is used only in non-FIPS mode. After that, the module returns to the FIPS Approved mode upon the removal of this card. Any operator that had previously been authenticated to the module in the FIPS Approved mode must re-authenticate after the module returns to the FIPS Approved mode. The module performs power up self-tests whenever it transitions from the non-FIPS Approved mode to the FIPS Approved mode.

The Zyt Cryptographic Module provides the current state of the module via the “Status” service.

FIPS Approved mode of operation

The cryptographic module supports the following FIPS Approved algorithms:

- RSA with 1024, 1536 or 2048 bit keys for digital signature generation and verification
- Triple-DES (two keys) for encryption
- SHA-1 for hashing

The Zyt Cryptographic Module relies on the implemented deterministic random number generator (DRNG) that is compliant with ANSI X9.31; a hardware NDRNG is used for seeding the Approved DRNG.

RSA with 1024, 1536 or 2048 bit keys is supported for key wrapping as a commercially available key establishment technique that meets the requirements of FIPS PUB 140-2 Annex D (key wrapping; key establishment methodology provides between 80 and 112 bits of encryption strength) (encryption of bulk data via RSA is only supported in the non-FIPS mode).

Non-FIPS mode of operation

In the non-FIPS mode, the cryptographic module supports all the algorithms implemented in the FIPS Approved mode and the following non-approved algorithms:

- RSA with 1024, 1536 or 2048 bit keys for encryption of bulk data (key wrapping; key establishment methodology provides between 80 and 112 bits of encryption strength)
- MD5 for hashing

4. Ports and Interfaces

The Zyt Cryptographic Module provides a single multi-pin connector that supports the following physical and logical interfaces:

- Main Power: receives main power via physically isolated pins on the multi-pin connector.
- USB: shared pins on the multi-pin connector for data input, data output, status, control.
- Interface to external liquid crystal display: shared pins on the multi-pin connector for status & data.
- Interface to external smart card: physically isolated pins on the multi-pin connector for dedicated data input, data output, status, control.
- Interface to external fingerprint sensor: shared pins on the multi-pin connector for data input, data output.
- Interface to external keypad: physically isolated pins on the multi-pin connector for control input.
- Interface to external battery: physically isolated pins on the multi-pin connector for backup power.
- Reset: physically isolated pins on the multi-pin connector for control.
- Wait: physically isolated pins on the multi-pin connector for control.

5. Identification and Authentication Policy

Assumption of roles

The Zyt Cryptographic Module shall support two distinct operator roles (User and Cryptographic-Officer). The Cryptographic Officer and the User are authenticated using an identity based authentication method. The operator is uniquely identified via an identity string (fingerprint template). The module authenticates the identity of the operator by verifying that the operator has possession of a unique valid TDES key. The role is explicitly selected with the first command issued after authentication of the operator.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	TDES Key
Cryptographic-Officer	Identity-based operator authentication	TDES Key

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Proof of possession of TDES key.	The probability that a random attempt will succeed or a false acceptance will occur is at most 1 in 2^80 which is stronger than the required minimum of 1 in 10^6. The probability of successfully authenticating to the module within one minute is less than 2^63 which is stronger than the required minimum of 1 in 10^5.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User: This role shall provide all of the services necessary for encryption and digital authentication of User data.	User Authentication: authenticates the authorized User role via proof of possession of a TDES key. Sign Data with RSA: digitally authenticate data entered into the USB port with RSA. Verify Data Signed with RSA: verify digitally authenticated data entered into the USB port with RSA. Zyt Card Management: creates and manages authentication parameters for Zyt smart cards. TDES Data Encryption: Encrypt data entered into the USB port with TDES. TDES Data Decryption: Decrypt data entered into the USB port with TDES. Hash Data: hash data received via the USB with SHA-1.
Cryptographic-Officer: This role shall provide all of the services necessary for secure management of	C.O. Authentication: authenticates the authorized C.O. role via proof of possession of a TDES key. Module initialization: initializes the cryptographic module.

the cryptographic module.	C.O. Get Status: returns status to the authenticated CO Zyt Card Management: creates and manages authentication parameters for Zyt smart cards Sign Data with RSA: digitally authenticates data entered into the USB port. Zyt Module Management: creates and manages the Zyt Module's keys. Hash Data: hash data received via the USB with SHA-1. Firmware Upgrade: loads new firmware onto the Zyt Module via RSA signature verification. C.O. Logoff: logs the C.O. off the system. Invalidate Zyt Module: brings the module back to a factory default state.

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services that do not provide key management functionality and do not use any Approved security functions:

- Initiate power-up self-tests: induced via power cycle.
- Zeroize: destroys all CSPs contained within the cryptographic boundary
- Unauthenticated Get Status: provides status of the device.
- Module Reset: resets the module; equivalent to power-cycle.
- Wait: slows down the communication speed of the cryptographic module to support interaction with slower peripheral equipment.
- Get Smart Card Reader State: retrieve status information from the peripheral smart card reader.
- Power smart card on/off: sends a command to the smart card reader to apply or remove power to/from the smart card's processor.
- Smart Card Reset: sends a command to reset the peripheral smart card's processor.
- Receive/transmit: receives and transmits plaintext data to and from the smart card reader.
- Get Date and Time: returns the date and time.
- Capture Fingerprint: retrieve a fingerprint image from the fingerprint port and send both the obtained image and quality information about this image out via USB.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- TDES Keys (TKs): used for TDES encryption/decryption
- RSA Signing Keys (RSKs): used for digital signature generation
- RSA Unwrapping Keys (RUKs): used for key unwrapping
- RNG Internal State (RIS): used for key generation, and random number generation

Definition of Public Keys:

The following are the public keys contained in the module:

- Manufacturer Public Key (MPK): Used to authenticate the firmware upgrade service via RSA digital signature verification.
- RSA Signature Verification Public Keys (RSVPKs): Used to verify RSA signatures.
- RSA Key Wrapping Public Keys (RKWPKs)**:** used for RSA key wrapping.

Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Use (U): the parameter is used within its corresponding cryptographic algorithm.
- Destroy (D): the parameter is zeroized.

Table 6 – CSP Access Rights within Roles & Services

Role		**Service**	**CSPs Access Operations**					**Public Key Access Operations**		
User	**C.O.**		**TKs**	**RSKs**	**PVKs**	**RIS**		**MPK**	**RSVPKs**	**RKWPKs**
X		User Authentication	U						U	
X		Sign Data with RSA	U	U	U	U				
X		Verify Data Signed with RSA							U	U

Role		**Service**	**CSPs Access Operations**					**Public Key Access Operations**		
User	**C.O.**		**TKs**	**RSKs**	**PVKs**	**RIS**		**MPK**	**RSVPKs**	**RKWPKs**
X		Zyt Card Management	U, D	U, D	U, D	U, D			U, D	U, D
X		TDES Data Encryption	U	U	U	U				
X		TDES Data Decryption	U	U	U	U				
	X	Hash Data								
	X	C.O. Authentication	U						U	
	X	Module initialization	U	U	U	U		U	U	U
	X	C.O. Get Status	U	U	U	U		U	U	U
	X	Sign Data with RSA	U	U	U	U				
	X	Zyt Module Management	U,D	U,D	U,D	U,D			U,D	U,D
	X	Hash Data								
	X	Firmware Upgrade						U		
	X	C.O. Logoff								
	X	Invalidate Zyt Module	D	D	D	D				
		Zeroize	D	D	D	D				
		Unauthenticated Get Status								
		Module Reset								
		Wait								

Role		Service	CSPs Access Operations					Public Key Access Operations		
User	C.O.		TKs	RSKs	PVKs	RIS		MPK	RSVPKs	RKWPKs
		Get Smart Card Reader State								
		Power smart card on/off								
		Smart Card Reset								
		Receive/transmit								
		Capture Fingerprint								

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the cryptographic module does not contain a limited operational environment, and does not support the loading or execution of untrusted code. Firmware upgrade integrity and authenticity is verified via RSA digital signature verification.

8. Security Rules

The Zyt Cryptographic Module's design corresponds to the Zyt 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 shall provide two distinct operator roles. These are the User role, and the Cryptographic-Officer role.
2. The cryptographic module shall provide identity-based authentication for all services that provide key management functionality and use Approved security functions. The cryptographic module also provides unauthenticated services that do not provide key management functionality and do not use Approved security functions.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. While in FIPS mode, the cryptographic module shall encrypt using the TDES algorithm, RSA for key wrapping only, RSA for digital signature generation/verification, SHA-1 for hashing, ANSI X9.31 for key generation.
5. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

1. Cryptographic algorithm tests:
    i. TDES Known Answer Test
    ii. DRNG Known Answer Test
    iii. SHA-1 Known Answer Test
    iv. RSA Known Answer Test (sign/verify & wrap/unwrap)
2. Firmware Integrity Test (SHA-1 hash verification)
3. Critical Functions Tests
    i. CPU ID check
    ii. Presence of Flash0 test (includes 32 bit CRC verification)
    iii. Presence of Flash1 test (includes 32 bit CRC verification)
    iv. Presence of Smart Card test
    v. Presence of USB test
    vi. CMOS Read/Write memory test (includes 32 bit CRC verification)

B. Conditional Self-Tests:

1. RSA sign/verify pairwise consistency test
2. RSA wrap/unwrap pairwise consistency test
3. Firmware load test via RSA signature verification
4. Continuous RNG test (on all implemented RNGs)

6. The operator shall be capable of commanding the module to perform the power-up self-test via power cycling the device.
7. Prior to each use, the internal RNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. The module shall not support concurrent operators.

9. Physical Security Policy

Physical Security Mechanisms

The Zyt Cryptographic Module is a multi-chip embedded cryptographic module that includes the following physical security mechanisms:

- Production-grade components
- Hard, opaque, tamper evident potting material encapsulation of multiple chip circuitry

enclosure. With very high probability, removal/penetration attempts will cause serious damage to the device, and render it non-functional.

Operator Required Actions

The operator is required to periodically inspect the device for tamper evidence as described below:

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard, opaque, tamper evident potting material encapsulation.	The cryptographic module is embedded within it's host device in a secure location during the manufacturing process under full control of Taua Biomatica. The cryptographic module is visually inspected by trusted Taua Biomatica employees before being sealed inside it's host unit. Further inspection for evidence of physical tampering on the cryptographic boundary is to be dictated by the cryptographic module owner's security policy.	Inspect the potting for evidence of a breach in physical security. If potting shows any signs of attempted physical access to underlying circuitry the device shall be destroyed.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate specific attacks outside the scope of FIPS 140-2.

Table 8 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

11. References

- FIPS PUB 140-2
- FIPS PUB 186-2
- FIPS PUB 180-1
- FIPS PUB 46-3
- ANSI X9.31

12. Definitions and Acronyms

- ANSI: American National Standards Institution
- C.O.: Cryptographic Officer
- CSP: Critical Security Parameter
- DRNG: Deterministic RNG
- FIPS PUB: Federal Information Processing Standard
- HSM: Hardware Security Module
- MD5: Message Digest 5
- MPK: Manufacturer Public Key
- NDRNG: Non-deterministic RNG
- RIS: RNG Internal State
- RNG: Random Number Generator
- RSA: Rivest-Shamir-Adelman algorithm
- RSKs: RSA Signing Keys
- RSVPKs: RSA Signature Verification Public Keys
- RUKs: RSA Unwrapping Keys
- SHA-1: Secure Hashing Algorithm – 1
- TDES: Triple Data Encryption Standard
- TKs: TDES Keys
- USB: Universal Serial Bus