Priva Technologies, Inc.

Priva Technologies Cleared IC Security Policy

Priva Technologies Inc.

Revision: 02 June 2005

TABLE OF CONTENTS

1. Module Overview

The Priva Technologies Cleared IC (HW P/N PC1002SC-2 Version 3.0, FW Version 4.0) is a single-chip cryptographic module used as an authentication and encryption device suited for transactions requiring security. The diagram below illustrates the cryptographic boundary of the chip, which is defined as the chip's outer perimeter:

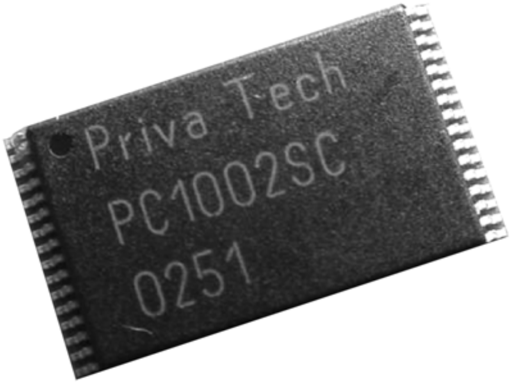

Figure 1: Image of the Priva Technologies Cleared IC

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

Approved mode of operation

The module operates in a FIPS Approved mode by default and indicates that it is in an Approved mode when the "Show Status" command is issued. Bit 23 of the chip status register indicates the mode of operation (0 = FIPS mode of operation). When the module is operated in a FIPS Approved mode, it supports the following FIPS Approved algorithm:

- Triple-DES (three key) in CBC mode

Non-Approved mode of operation

The module also supports a non-Approved mode of operation. When an operator utilizes the module in the "Vendor Secure Mode", the module is operating in a non-Approved mode and will indicate the non-Approved mode of operation by setting bit 23 of the chip status register to 1. The cryptographic module also supports the following non-Approved algorithms:

- MD5 (only used in the non-Approved mode)
- NDRNG (The module supports an NDRNG that is used to generate random non-security relevant values; the Priva Technologies Cleared IC does not support key generation.)

4. Ports and Interfaces

The Priva Technologies Cleared IC supports a data input, data output, control input, status output, and a power interface. All interfaces supported by the Priva Technologies Cleared IC are provided by the module's physical 32-pins.

5. Identification and Authentication Policy

Assumption of roles

The Priva Technologies Cleared IC supports two distinct operator roles: a User and Cryptographic Officer. The cryptographic module enforces the separation of roles using identity-based operator authentication. The User role is authenticated by providing the unique 128-bit User ID and by proving knowledge of a 192-bit shared secret. The Cryptographic Officer is identified by providing the unique 64-bit CO ID and by proving knowledge of a 192-bit shared secret. Upon correct authentication, the role is selected based on the authentication information of the operator. The Priva Technologies Cleared IC does not retain any previous authentications across power cycles and does not provide any feedback information during authentication.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Unique 128-bit User ID and knowledge of 192-bit shared secret (Private Key 3)
Cryptographic Officer	Identity-based operator authentication	Unique 64-bit CO ID and knowledge of 192-bit shared secret (Private Key 1)

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Knowledge of 192-bit Shared Secret	The probability that a random attempt will succeed or a false acceptance will occur is the inverse of 2^112 which is less than 1/1,000,000. The module allows four successive failed authentication attempts before the module must be reinitialized via power cycling for USB. After 64 successive failed authentication attempts, the module is zeroized and becomes inoperable. The maximum amount of attempts to authenticate in a one-minute period is 64 and the probability that an attempt will succeed in a one minute period is 64/2^112, which is

	less than 1/100,000.

6. Access Control Policy

The following services are provided to the User and Cryptographic Officer:

Table 4 – Services Authorized for Roles

Services	**User**	**Crypto Officer**
Write User Information: An unlocked Priva Technologies Cleared IC allows the user or the Crypto Officer to modify User information, such as the User ID.	X	X
Session Load: This function loads session information and settings once the Priva Technologies Cleared IC and the CO have successfully authenticated each other. This service also loads the Session Key.		X
Stream Key Load: This function loads the Stream Key to be used for data encryption/decryption during streaming services. This also enables a streaming session.		X
Encrypt Data: This function takes plaintext data and encrypts it using the predefined secret keys loaded prior to this command.	X	X
Decrypt Data: This function takes encrypted data and decrypts it using the predefined secret keys loaded prior to this command.	X	X
Zeroization: Zeroization is the function utilized to actively overwrite all volatile and non-volatile memory with zeroes; This ensures that all plaintext CSPs are		X

zeroized.		

The following services do not require any user authentication and do not access any CSPs:

Show Status: Show the status information of the module. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

Set LED: Allows an operator to set the rate at which an externally connected LED blinks. Alternatively, the operator may turn the externally connected LED off or set it to remain constantly on. Upon power cycling the module, the extermally connected LED will return to blinking at its default rate.

Self-Tests: Power-up Self-Tests are invoked by power cycling the module and may be invoked at any time. The externally connected LED blinking at a constant rate shall indicate successful completion of self-tests.

Secure Priva Technologies Cleared IC: This function logs out any users currently logged into the module; resets all unlock flags; and clears local, management, and application flags.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Session Key – TDES key used to encrypt session data
- Stream Key – TDES key used to encrypt streaming data.
- Private Key 1 – TDES key used to authenticate the CO role.
- Private Key 2 – TDES key used to decrypt the Session Key.
- Private Key 3 – TDES key used to authenticate the User role.

Definition of CSPs Modes of Access

Table 5 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: Crypto module performs crypto services using the TDES keys specified prior to the command.
- Zeroize: The crypto module actively overwrites all CSPs in volatile and non-volatile memory with zeroes.
- Load: This operation loads TDES keys into the crypto module TDES encrypted.

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
X	X	Write User Information	Use Session Key
X		Session Load	Load Session Key Use Private Key 2
X		Stream Key Load	Load Stream Key Use Session Key
X	X	Encrypt Data	Use Session Key Use Stream Key
X	X	Decrypt Data	Use Session Key Use Stream Key
X		Zeroization	All CSPs

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Priva Technologies Cleared IC does not support a modifiable operational environment.

8. Security Rules

The Priva Technologies Cleared IC'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: the User and the Cryptographic-Officer role.
2. The cryptographic module provides identity-based authentication.
3. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
4. The cryptographic module encrypts message traffic using the TDES algorithm.
5. The cryptographic module shall perform the following tests:

A. Power-Up Self-Tests

   i. Cryptographic Algorithm Tests

      1. TDES Known Answer Tests

   ii. Software/Integrity Test – N/A. Firmware image is masked into ROM.

   iii. Critical Functions – None.

B. Conditional Tests – N/A.

7. The externally connected LED being constantly on after a power-up shall indicate failure of the TDES KAT.
8. The module does not support key generation or manual key entry.
9. The module does not support a bypass capability.
10. The module inhibits all data output during self-tests, zeroization, and error states.
11. The module supports concurrent operators.
12. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9. Physical Security Policy

Physical Security Mechanisms

The Priva Technologies Cleared IC cryptographic module includes the following physical security mechanisms:

- Production-grade components.
- Hard potting material used to encapsulate the single chip circuitry with removal/penetration attempts causing evidence of tamper and severely damaging the internal circuitry of the chip.

Operator Required Actions

The Cryptographic Officer is required to zeroize the Priva Technologies Cleared IC when there is suspicion of tamper or theft.

10. Mitigation of Other Attacks Policy

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

11. Definitions and Acronyms

PSI	Priva Serial Interface (Priva's Proprietary version of SPI)
TDES	Triple Data Encryption Standard
KAT	Known Answer Test
ROM	Read-Only Memory
CSP	Critical Security Parameter
CO	Cryptographic Officer
NC	No Connect
NDRNG	Non-Deterministic Random Number Generator