SecureToken ST3 Security Target

Common Criteria: EAL1

Version 1.0

19-JAN-2011

Document management

Document identification

Document ID	ST3_EAL1_ASE
Document title	SecureMetric SecureToken ST3 Security Target
Product version	Version 1.0

Document history

Version	Date	Description
0.1	27-JUL-10	Release for internal review.
0.2	29-JUL-10	Updated to address internal comments
0.3	06-AUG-10	Updated SecureCOS to SecureCOS 2.
0.4	19-NOV-10	Updated to address EORs
0.5	23-NOV-10	Addressed evaluators' comments
1.0	19-JAN-11	Final ETR.

Table of Contents

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	SecureMetric SecureToken ST3 Security Target
ST Version	1.0, 19-JAN-2011
TOE Reference	SecureToken ST3
TOE version	Version 1.0
Assurance Level	EAL1
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; • Part Three – Security Assurance Components, Revision Three, July 2009.

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST as well as the TOE description including the physical and logical scope of the TOE.
- Section 2 provides the conformance claims for the evaluation.
- Section 3 defines the security objectives for the environment.
- Section 4 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.
- Section 5 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE
- Section 6 provides the glossary for the ST.

1.3 TOE Overview

1.3.1 TOE type and usage

The SecureMetric SecureToken ST3 product provides a number of capabilities designed to support organisations in rapidly developing and deploying enterprise PKI-related security solutions.

The product provides:

- a USB token embedded with a security ICC that is embedded with the SecureCOS and offers core PKI-related cryptographic functions;
- a software development kit (SDK) with source and headers files that can be used to support the development of applications;
- a range of utilities and token management applications that resides on a host PC; and
- a suite of middleware binaries that provide compiled APIs that serve as an interface to the token and associated security functionality (these also reside on the host PC).

The TOE comprises core components of the SecureMetric SecureToken ST3 product and is confined to the following three main components of the product:

- **SecureCOS operating system.** The operating system (firmware) embedded on the token ICC. The operating system provides the core cryptographic functionality of the TOE.
- **SecureCOS Middleware.** Two compiled binaries that provide exported APIs to provide an interface to the core cryptographic security functionality of the TOE, providing developer's with an easily accessible method for engaging PKI-related functionality to support the development of enterprise authentication and integrity solutions.
- **SecureCOS Token Management Tools.** The TOE provides two specific applications, one for the SO (administrator) and the second for the user, to manage the key security functionality of the TOE.

The TOE is referred to as SecureToken ST3 in this document.

1.3.2 TOE Life-cycle

The general life-cycle of a smart card product, as defined in [PP/BSI-0002], is split up into 7 phases as described below:

- **Phase 1 Smart Card software development.** The SW developer is responsible for the development of the OS (SecureCOS) and the application.

- **Phase 2 IC design, IC database construction and IC photomask fabrication.** The IC manufacturer is responsible for these operations, taking as an input the embedded software data given by SW developer.

- **Phase 3 IC manufacturing and testing.** The IC manufacturer is responsible for producing and testing the IC through three main steps: IC manufacturing, testing, and IC pre-personalization.

- **Phase 4 Module assembling and packaging.** The smart card product manufacturer is responsible for assembling the module.

- **Phase 5 Smart card pre-personalization.** The smart card product manufacturer is responsible for the smart card initialization, for installing the application (if needed) and for testing, and the smart card pre-personalization.

- **Phase 6 Smart card Personalization.** The Personalizer is responsible for the personalization of the application. The application can also be installed in this phase.

- **Phase 7 Smart card Usage.** The smart card issuer is responsible for the smart card product delivery to the smart card end-user, and for the end

The TOE is the end product at the end of phase 5. The design of the TOE is at phase 1 and the initialization of the TOE is done in phase 5.

1.3.3 TOE security functions

The following table highlights the range of security functions and features implemented by the TOE.

Security function	Description
Cryptographic Operations	The TOE provides a cryptographic library for cryptographic operations that can be used by applications outside the TOE.
User Authentication	Access to the TOE management functions needs authentication by user and administrator using their respective passphrase (PIN). After 3 times of failed authentication by the user, the accessibility to the token will be blocked and the administrator PIN is needed to unblock the token (resetting the user PIN).
Security Management	The TOE provides management functions such as changing PIN, creation of user.

1.4 TOE Description

1.4.1 Physical scope of the TOE

The TOE comprises the SecureToken ST3 operating system SecureCOS, middleware and the SecureCOS Token Management Tools. SecureCOS is embedded into the memory of the underlying security IC. The middleware and the Token Management tools are installed onto a host PC for development platforms to communicate with SecureCOS and to manage the key security functionality of the TOE. The architecture of the TOE is shown in figure 1 below.

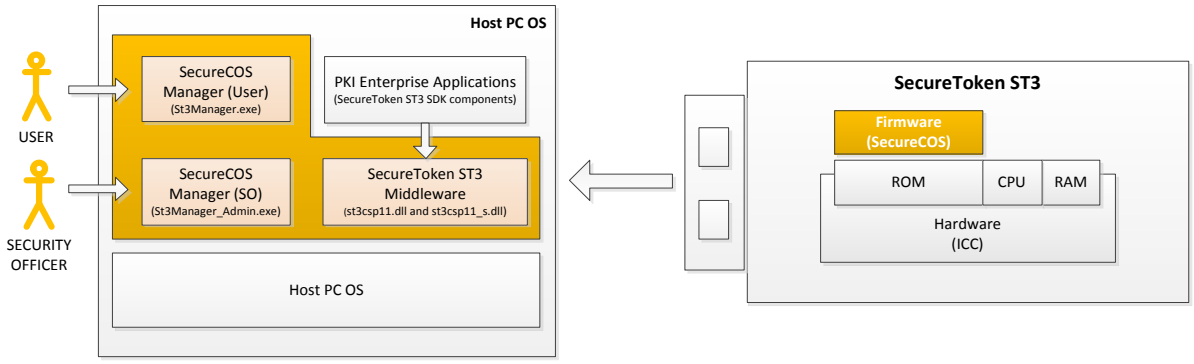

Figure 1 – TOE architecture

The table below shows the versions and descriptions of the TOE components.

TOE Component	Description
SecureCOS	The operating system (firmware) embedded on the token ICC. The operating system provides the core cryptographic functionality of the TOE.
SecureToken ST3 Middleware (st3csp11.dll and st3csp11_s.dll)	Two compiled binaries that provide exported APIs to provide an interface to the core cryptographic security functionality of the TOE, providing developer's with an easily accessible method for engaging PKI-related functionality to support the development of enterprise authentication and integrity solutions.
SecureToken ST3 Token Managers (ST3manager.exe and ST3manager_admin.exe)	The TOE provides two specific applications, one for the SO (administrator) and the second for the user, to manage the key security functionality of the TOE.

The underlying hardware and software that is used to support the TOE are:

- Any processor running the following platform:
    - Windows 98 SE
    - Windows Me
    - Windows 2000
    - Windows XP
    - Windows 2003
    - Windows Vista
- A USB port available on the computer and the BIOS supports USB devices, and the USB support feature in CMOS settings is enabled
- SecureToken ST3 hardware token with pre-installed SecureCOS.

1.4.2 Logical scope of the TOE

The logical boundary consists of the security functionality of TOE is summarized below.

- **User Authentication.** User and the administrator of the token authenticate themselves to the TOE using their PINs. The TOE will only allow access to the TOE functions and resources after a successful authentication. After 3 times of failed authentication by the user, the accessibility to the token will be blocked and the administrator PIN is needed to unblock the token (resetting the user PIN).
- **Cryptographic Operation.** The TOE cryptographic library includes 3-DES, RSA, MD5 and SHA-1 that applications can use for their specific purpose.
- **Security Management.** The TOE maintains 2 roles to ensure that functions are restricted to those who have the privilege to access them. The roles maintained by the TOE are the user of the SecureToken ST3 and the administrator. Only the administrator can unblock the token for the user when the user is blocked when exceeding the number of authentication failure by the user.

2 Conformance Claim (ASE_CCL)

The ST and TOE are conformant to version 3.1 (Revision 3) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 3.

- Part 3 conformant, EAL1. Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3. Evaluation is EAL1

3 Security objectives (ASE_OBJ)

3.1 Overview

The security objectives at an EAL1 level of assurance include concise statements of the objectives to be achieved by the supporting environment.

3.2 Security objectives for the environment

Identifier	Objective statements
OE.CHIP	The security IC upon which the TOE resides must: • maintain the integrity and the confidentiality of the content of the Security IC memories as required by the context of the TOE; • maintain the correct execution of the TOE; • have measures to protect itself on the operations of the IC (physical security, detection of out-of-range supply voltages, frequencies, or temperatures, detection of illegal addressing or instructions); and • have measures to protect itself against leakage of information from the IC.
OE.INSTALL	The TOE shall be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures and only by trustworthy IC and Product Manufacturers.
OE.ENVIRONMENT	The sites of the IC and Product manufacturers are physically secure sites. The development or manufacturing process is well documented with proper configuration management systems. The staffs at these sites are well-trained to handle the TOE securely.

4 Security requirements (ASE_REQ)

4.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

4.2 SFR conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

4.3 Security functional requirements

4.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 4.2 and summarized in the table below.

Identifier	Title
FCS_CKM.1a	Cryptographic key generation (TDES)
FCS_CKM.1b	Cryptographic key generation (RSA)
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1a	Cryptographic Operation (TDES)
FCS_COP.1b	Cryptographic Operation (RSA)
FCS_COP.1c	Cryptographic Operation (SHA)
FCS_COP.1d	Cryptographic Operation (MD5)
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FMT_MTD.1a	Management of TSF data (user PIN)
FMT_MTD.1b	Management of TSF data (Admin PIN)
FMT_MTD.1c	Management of TSF data (block status of user)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles

4.3.2 FCS_CKM.1a Cryptographic key generation (TDES)

Hierarchical to:	No other components.
FCS_CKM.1a.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**TDES**] and specified cryptographic key sizes [**128 bits**] that meet the following: [**Annex E.4.1 of [GP211].**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

4.3.3 FCS_CKM.1b Cryptographic key generation (RSA)

Hierarchical to:	No other components.
FCS_CKM.1b.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA key generation**] and specified cryptographic key sizes [**1024 and 2048 bits**] that meet the following: [**RSA PKCS#1**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

4.3.4 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: [**overwrite the keys**] that meets the following: [**no standard**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Notes:	None.

4.3.5 FCS_COP.1a Cryptographic Operation (TDES)

Hierarchical to:	No other components.
FCS_COP.1a.1	The TSF shall perform [**TDES encryption and decryption**] in accordance with a specified cryptographic algorithm [**TDES-CBC, TDES-EBC**] and cryptographic key sizes [**112 bits for TDES 2 keys, 168 bits for TDES 3 keys**] that meet the following: [**FIPS 46-3**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

4.3.6 FCS_COP.1b Cryptographic Operation (RSA)

Hierarchical to:	No other components.
FCS_COP.1b.1	The TSF shall perform [**RSA encryption and decryption**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**1024 and 2048 bits**] that meet the following: [**RSA PKCS#1**]**.**
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

4.3.7 FCS_COP.1c Cryptographic Operation (SHA)

Hierarchical to:	No other components.
FCS_COP.1c.1	The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-2**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

4.3.8 FCS_COP.1d Cryptographic Operation (MD5)

Hierarchical to:	No other components.
FCS_COP.1d.1	The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**MD5**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-2**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

4.3.9 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [***3***] unsuccessful authentication attempts occur related to [**user entering their passphrase (PIN) for authentication to the TOE**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**block the user usage of the TOE**].
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.10 FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**stored user/administrator PIN]**
Dependencies:	No dependencies.
Notes:	User PINs are the only attributes maintained by the TOE in the context of this requirement.

4.3.11 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.3.12 FMT_MTD.1a Management of TSF data (user PIN)

Hierarchical to:	No other components
FMT_MTD.1a.1	The TSF shall restrict the ability to [***modify***] the [**User PIN**] to [**User**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None

4.3.13 FMT_MTD.1b Management of TSF data (Admin PIN)

Hierarchical to:	No other components
FMT_MTD.1b.1	The TSF shall restrict the ability to [***modify***] the [**Administrator PIN**] to [**Administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

4.3.14 FMT_MTD.1c Management of TSF data (block status of user)

Hierarchical to:	No other components
FMT_MTD.1c.1	The TSF shall restrict the ability to [***modify***] the [**userBlock**] to [**Administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	The administrator can reset the userBlock so that user can use the TOE again after being blocked. This is done by changing the field to No and resetting the user PIN.

4.3.15 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) creation of users with default passwords** **b) changing of passwords** **c) reset block status of user** **d) import, export, delete digital certificate**]
Dependencies:	No dependencies.
Notes:	The administrator can reset the userBlock so that user can use the TOE again after being blocked. This is done by changing the field to No and resetting the user PIN.

4.3.16 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**Administrator, Users**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

4.4 Dependency analysis

SFR	Dependency	Inclusion
FCS_COP.1a	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1a FCS_CKM.4
FCS_COP.1b	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1b FCS_CKM.4
FCS_COP.1c	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	None. No keys are needed for hashing
FCS_COP.1d	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	None. No keys are needed for hashing
FCS_CKM.1a	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1a FCS_CKM.4
FCS_CKM.1b	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1b FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1a FCS_CKM.1b

SFR	Dependency	Inclusion
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FIA_ATD.1	No dependencies	NA
FIA_UAU.2	FIA_UID.1 Timing of identification	None. There are only 2 users for the TOE. As administrator and a user. There are identified by the interfaces where the users use for authentication.
FMT_MTD.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1c	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	None. There are only 2 users for the TOE. As administrator and a user. There are identified by the interfaces where the users use for authentication.

4.5 TOE security assurance requirements

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 1 (EAL1).

EAL1 provides a basic level of assurance by a limited security target and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behavior.

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

This EAL provides a meaningful increase in assurance over unevaluated IT.

Assurance class	Assurance components
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.1 TOE CM coverage
	ALC_CMC.1 Labelling of the TOE
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

5 TOE summary specification (ASE_TSS)

5.1 User Authentication

Administrator and user of the TOE can authenticate to the TOE through an application, Token Manager which is outside the scope of evaluation. The Token Manager provides an interface to access management functions.

Administrator and user need to present their PIN to the TOE for authentication. Only after a successful authentication will the TOE allows the users to access the TOE functions. (FIA_UAU.2)

The TOE maintains the status of the authentication by changing the authenticity value of the users to True if the administrator or user is successfully authenticated. The default value of the authenticity value is always false otherwise. (FIA_ATD.1)

As there are only 2 users to the TOE, the TOE identifies the user by checking the PIN of the user. Administrator enters the SO PIN whereas user will enter the USER PIN. The interfaces for the authentication for administrator and user are different so that the TOE will know if the authentication is for the administrator or the user.

Only the administrator is able to unblock the token when the token is in the block state. The block state comes about when user enters his/her PIN wrongly for 3 times. When this happens, the TOE will prevent all access and operations to the TOE for the user.

To unblock, the administrator will have to authenticate to the TOE. The TOE will check the authenticity of the administrator. If the administrator is successfully authenticated and the authenticity value of the administrator is set to True, then the TOE will allow the administrator to unblock the token. (FIA_AFL.1)

5.2 Cryptographic Operation

The TOE performs RSA, Triple Des, SHA-1 and MD5 operations. (FCS_COP.1a, FCS_COP.1b, FCS_COP.1c, FCS_COP.1d) It also provides key generation for RSA and TDES (FCS_CKM.1a, FCS_CKM.1b) and key destruction by overwriting the memory space of the key (FCS_CKM.4).

These operations are used by applications on the host system. The applications must comply with PKCS#11 and CSP standards and use the middleware of the TOE to access these functionalities provided by the TOE.

5.3 Security Management

The TOE maintains 2 roles. They are user and administrator (FMT_SMR.1). Below shows the management functions available to user and administrator (FMT_SMF.1, FMT_MTD.1a, FMT_MTD.1b, FMT_MTD.1c).

- creation of users with default passwords (administrator)
- changing of passwords (user, administrator)
- unblock token (administrator)
- import, export, delete digital certificate (user)

6 Glossary

Term	Description
Administrator	A user authorized to perform TOE personalisation, or other TOE administrative functions. In the ST, administrator is also called Security Officer.
Authentication Data	It is information used to verify the claimed identity of a user.
Cipher-block chaining (CBC)	In the cipher-block chaining (CBC) mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted.
Electronic codebook (ECB)	The message is divided into blocks and each block is encrypted separately.
FIPS 46-3	It is a Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology for DATA ENCRYPTION STANDARD.
GP211	Global Platform Card Specification – v2.1.1, March 2003.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
MD5	MD5 (Message-Digest algorithm 5) is a cryptographic hash function with a 128-bit hash value.
Personalisation	The process by which personal data are brought into the TOE before it is handed to the card holder.
PIN	It is a secret numeric password shared between a user and a system that can be used to authenticate the user to the system.
PKCS#1	It is the first of a family of standards called Public-Key Cryptography Standards (PKCS), published by RSA Laboratories. It provides the basic definitions of and recommendations for implementing the RSA algorithm for public-key cryptography.

Term	Description
RSA	It is an algorithm for public-key cryptography.
SmartCard	A credit card sized chip card with embedded integrated circuits. Often used to store keys for authentication.
SHA-1	It is a cryptographic hash function designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. It produces a 160-bit hash value.
TDES	It is a block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE
User	It means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user, that does not affect the operation of the TSF