ISO/IEC 15408
Information Technology Security Evaluation

Hitachi Software Engineering Co., Ltd.

Smart Folder 3 Security Target

Author(s): Toru Miyazawa, Hideyuki Sugawara
Date: January 6, 2004
Version: 2.19

Document Version

This document is written and managed as the following list:

Version	Date	Author(s)	Comment
0.1	Sep. 10, 2001	Toru Miyazawa	Initial draft version
1.0	Nov. 20, 2001	Toru Miyazawa	Initial version
1.1	Jan. 30, 2002	Toru Miyazawa	Evaluated
2.0	Apr. 22, 2002	Toru Miyazawa	TOE functional design change
2.1	Jun. 24, 2002	Toru Miyazawa	Evaluated and product name changed to "Smart Folder 3"
2.2	Sep. 3, 2002	Hideyuki Sugawara	Evaluated and product components changed to "Smart Folder 3" Fixed following ORs
2.3	Oct. 2, 2002	Hideyuki Sugawara	Fixed following ORs
2.4	Jan. 15, 2003	Hideyuki Sugawara Toru Miyazawa	Fixed following ORs
2.5	Jan. 31, 2003	Hideyuki Sugawara Toru Miyazawa	Fixed following ORs
2.6	Feb. 25, 2003	Hideyuki Sugawara Toru Miyazawa	Fixed following ORs
2.7	May 19, 2003	Hideyuki Sugawara Toru Miyazawa	Fixed following ORs
2.8	Jul. 9, 2003	Hideyuki Sugawara Toru Miyazawa	Fixed following ORs
2.9	Jul. 11, 2003	Hideyuki Sugawara Toru Miyazawa	Fixed following ORs
2.10	Aug. 7, 2003	Hideyuki Sugawara Toru Miyazawa	Fixed following ORs
2.11	Aug. 21, 2003	Hideyuki Sugawara	Fixed following ORs
2.12	Aug. 28, 2003	Hideyuki Sugawara	Fixed following ORs
2.13	Nov. 5, 2003	Hideyuki Sugawara	Fixed following ORs
2.14	Nov. 17, 2003	Hideyuki Sugawara	Fixed following ORs
2.15	Nov. 25, 2003	Hideyuki Sugawara	Fixed following ORs
2.16	Dec. 1, 2003	Hideyuki Sugawara	Fixed following ORs
2.17	Dec. 5, 2003	Hideyuki Sugawara	Fixed following ORs

Version	Date	Author(s)	Comment
2.18	Jan. 5, 2004	Hideyuki Sugawara	Fixed following ORs
2.19	Jan. 6, 2004	Hideyuki Sugawara	Fixed following ORs

Table of Contents

1. ST Introduction

1.1. ST Identification

Title:	Smart Folder 3 Security Target
ST version:	2.19
TOE name:	Smart Folder 3 MULTOS application
TOE version:	03-06
Author(s):	Toru Miyazawa, Hideyuki Sugawara
Date:	January 6, 2004
CC version:	ISO/IEC 15408-1, First edition 1999-12-01
	ISO/IEC 15408-2, First edition 1999-12-01
	ISO/IEC 15408-3, First edition 1999-12-01
Assurance level:	EAL4

Keywords: Smart Card, PKI, private key, digital certificate, digital signature, encryption, security, Crypto API, PKCS#11, Certificate Authority (CA), Registration Authority (RA)

1.2. Glossary of Terms

No.	Term	Description
1.	PKI (Public Key Infrastructure)	This is a security infrastructure for IT system using public key technology. Well known security systems, such as Digital certificates, digital signature and encryption, are all included in the infrastructure.
2.	Smart Folder 3	Smart Folder 3 is a component of applications for PKI smart card access. This includes an issuer tool library, a user tool, an administrator tool and a MULTOS application (TOE).
3.	Cooperating PC software	This includes PC tools that cooperate with the TOE: Issuer tool library, Administrator tool and normal user tool.
4.	MULTOS smart card	This is a HITACHI MULTOS 4.06 smart card (Chip version AE45C).
5.	MULTOS OS	This is an operating system that runs on MULTOS smart card.
6.	MULTOS application	This is an application that runs on MULTOS OS. The TOE is one of the MULTOS applications.
7.	MULTOS chip	This is an IC chip on which MULTOS OS and MULTOS applications run.

No.	Term	Description
8.	Microsoft smart card logon	Operating system logon using smart card supported by the Windows 2000/XP. An optional component is required to realize the Microsoft smart card logon in Windows NT4.0/98/98SE. This is not required for the TOE to run.
9.	Web authentication	Personal identification on the internet using the PKI.

1.3. ST Overview

This security target (ST) is for the Smart Folder 3 MULTOS application.

The Smart Folder 3 MULTOS application is a security application that stores PKI keys and Digital certificates in MULTOS smart card securely. PKI keys can be generated in a MULTOS smart card using the application. In this case, PKI private key will never go out of the MULTOS smart card. PKI Keys can also be generated outside of MULTOS smart card and imported to it.

TOE is guarded by PIN authentication function. The TOE recognizes a user, who entered a correct PIN, as an authorized owner of the TOE. And the TOE will be locked after defined number of consecutive wrong PIN inputs. The TOE has a re-authentication function, which requires another authentication for signing and decrypting operations even if the user has been authenticated.

1.4. CC Conformance Claim

The TOE is:

1. CC Part2 conformant
2. CC Part3 EAL4 conformant

2. TOE Description

This section describes the TOE by identifying the product type and the TOE boundaries.

2.1. TOE Overview

The TOE of this ST is the Smart Folder 3 MULTOS application. It is an application for the MULTOS OS

2.1.1. Target User

Smart Folder 3 users can use MULTOS smart card for PKI security system. The PKI security system includes:

1. Access control for intranet systems
2. Access control for B to B systems
3. E-mail Encryption systems

2.2. Product Type

Product type of Smart Folder 3 is a component of applications for PKI smart card access. And product type of TOE is an application that keeps PKI private keys safe and controls access of PKI private key.

2.2.1. Product Components

The product can be distributed as one of the following units:

1. The Issuer tool library

   A MULTOS smart card issuing center uses this tool to initialize MULTOS smart card and distribute them to users. This is provided as a library so the center can customize the tool and it will fit the center’s operation procedures and facilities.

2. The Administrator tool

   This tool is for MULTOS smart card administrators. The administrators provide services for MULTOS smart card users. The service includes unlocking normal user PIN locked MULTOS smart card.

3. The User tool

   The user tool is a user interface to the TOE. A user logs onto the TOE using the tool.

   Users can use the Microsoft Internet Explorer or the Netscape Navigator/Communicator to access a Web system requiring SSL client authentication. They can use the Microsoft Outlook Express or the Netscape Messenger to send/receive signed and encrypted E-mails.

4. The MULTOS application

   This is the TOE of this ST. It runs on a MULTOS smart card. It stores PKI keys and Digital certificates and operates decryption and digital signature generation functionalities. Note that the generation of a signature function and the decryption function are not TSF. It is protected by a PIN authentication function of the TOE and this function is the TSF. PIN authentication function is a function, which compares the PIN inputted by Administrator/Normal user on cooperating PC,

corresponds to the PIN kept in the TOE. When an inputted PIN and the PIN stored in the TOE matches, the user can logon to the TOE and the user can perform the operations which are permitted for normal users. When the PINs are different, the user cannot logon. The TOE will be locked after defined number of consecutive wrong PIN inputs and further authentication requests are rejected.

Thus, Normal user PIN required to access the PKI key is actually a TSF data. The definition of user data and TSF data is at Figure 4 TOE Objects of 2.4 Objects.

The TOE is loaded onto the MULTOS smart cards before arriving at issuers' sites. Only one issuer tool library and one administrator tool are necessary for a whole system while the user tool must be installed on every user PC and the MULTOS application is needed for every MULTOS smart card.

The TOE is verified to run under the environment shown below:

1. MULTOS smart card
   - MULTOS OS: HITACHI MULTOS 4.06
   - Chip: AE45C

Hardware, Software and peripherals that are connected to the TOE are shown below:

2. Cooperate PC (issuer tool library, administrator tool)
   - Hardware: AT compatible
   - OS: Microsoft Windows 2000 / NT 4.0
   - Browser / Mailer:
     - Netscape Navigator / Communicator 4.75
     - Microsoft Internet Explorer 5.0
3. Cooperate PC (normal user tool)
   - Hardware: AT compatible
   - OS: Microsoft Windows 2000 / NT 4.0 / 98 /98SE
   - Browser / Mailer:
     - Netscape Navigator / Communicator 4.75
     - Microsoft Internet Explorer 5.0
4. Smart card Reader / Writer
   - PC/SC compliant smart card Reader / Writer

2.2.2. Product Lifecycle

The TOE must be loaded onto a MULTOS smart card by a MULTOS issuer because the TOE is a MULTOS application. This MULTOS application load process, which is

operated by a MULTOS issuer, is outside of the scope of this ST. This ST handles the TOE after it is loaded onto a MULTOS smart card. A typical TOE lifecycle is shown below:

The TOE is not in issued state when it is loaded onto a MULTOS smart card. An issuer determines initial values for the TOE objects (e.g. defines an initial normal user PIN and generates and/or imports PKI keys and Digital certificates, when necessary) and issues MULTOS smart card using the issuer tool library. After the MULTOS smart card is issued, one cannot modify the initial PIN, PKI keys and Digital certificates using the issuer tool library.

The issuer delivers an issued MULTOS smart card to a normal user. The normal user changes the initial PIN, which the issuer set, to a new PIN (i.e. permanent PIN). The normal user can use the TOE to change the PIN, store PKI keys and Digital certificates and generate PKI keys and Digital certificates. The TOE can hold two pairs of PKI keys at the maximum and normal user can delete or overwrite PKI keys when the PKI keys become unnecessary. When normal user inputs wrong PINs issuer-defined times consecutively, the TOE is normal user PIN locked. In this case, normal user brings the TOE to an administrator and asks the administrator to unlock the TOE.

The administrator logs on to the TOE as an administrator and unlocks the TOE. And then the administrator gives the TOE back to the normal user.

When normal user does not use the TOE anymore, the normal user brings the MULTOS smart card to an administrator. Administrator can logs on to the TOE and initialize it. After this initialization, administrator gives the TOE to an issuer. The TOE is in exactly the same state as an unused TOE. So, the issuer can re-issue the TOE and give it to another normal user.

2.3. TOE Boundary

2.3.1. TOE Physical Boundary

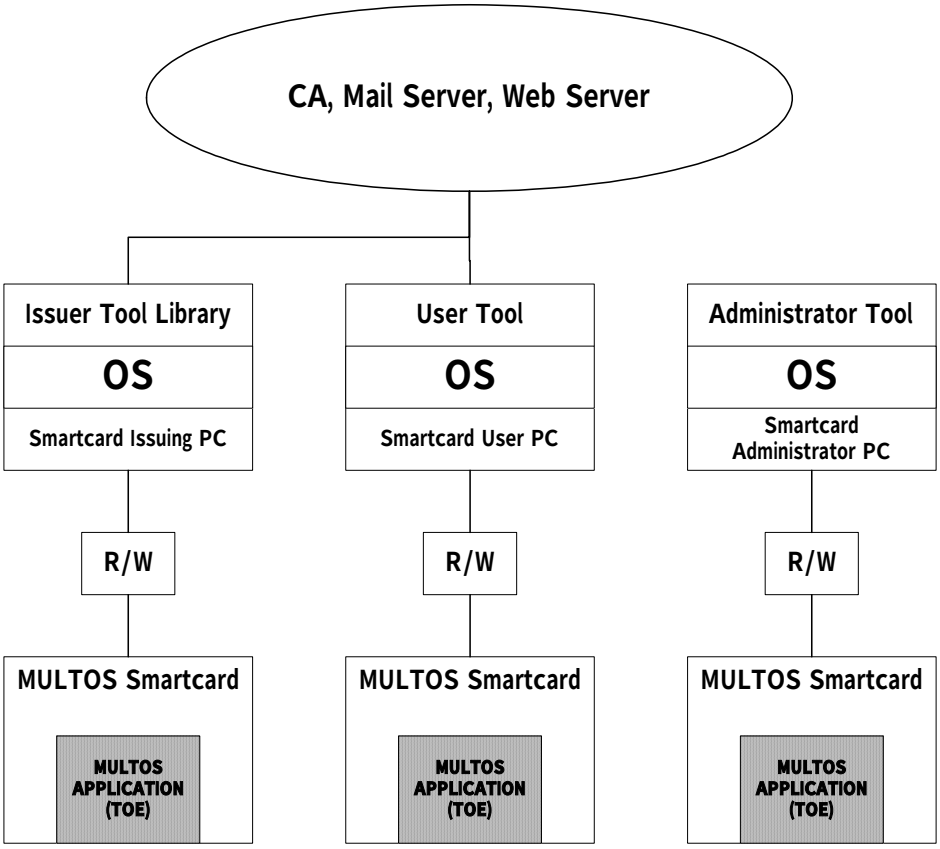

Figure 1 TOE Physical Boundary

Figure 1 shows a sample physical image of security system including the TOE. The TOE of this ST is shadowed.

Issuer tool library and User tool can connect to CA (Certification Authority), Mail Server and Web Server. Administrator tool is not necessary to be connected to CA, because an administrator only unlocks a Normal user PIN locked MULTOS smart card and initialize MULTOS smart card. In this process, CA, Mail Server, Web Server is not necessary.

The TOE of this ST only includes the Smart Folder 3 MULTOS application. All other products (e.g. CA, OS, R/W, each PC, the user tool, the administrator tool and issuer tool library) are not included in the TOE.

The TOE runs on a HITACHI MULTOS 4.06 smart card. The MULTOS smart card has a processing unit and an operating system called MULTOS OS. All of these MULTOS smart card components are excluded from the TOE.

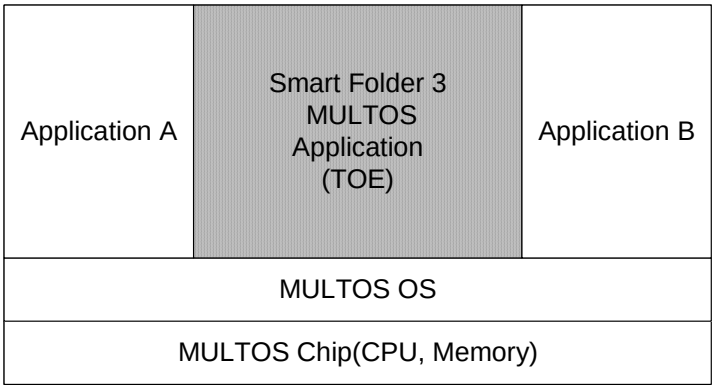

Figure 2 Inside MULTOS Smart card

Figure 2 shows a simplified structure of the MULTOS smart card, in which the Smart Folder 3 MULTOS application is loaded. The TOE of this ST is only the Smart Folder 3 MULTOS application (shadowed in Figure 2). The MULTOS smart card itself and all other applications coexisting in the same MULTOS smart card are not part of the TOE.

The MULTOS smart card is a smart card. MULTOS smart card can be considered as a tiny computer. It is small but it has the same functions as computers. The computer has a CPU to calculate/process data/programs and stores the data/programs in its memory. The MULTOS smart card has exactly the same components. It has its own CPU and memory. Of course, it can store data. In addition, it can execute programs. The normal computer runs an operating system (OS). The most famous OS for PC is Microsoft Windows. The MULTOS smart card has its own OS, too. Various user applications can run on the OS. The Smart Folder 3 MULTOS application, which is the TOE of this ST, is one of these user applications. It runs on the MULTOS OS. Other user applications may exist on the same MULTOS smart card. But these applications cannot affect other applications loaded on the same MULTOS smart card. The MULTOS OS ensures this by providing firewalls between loaded user applications. So, in this ST, we do not have to care about malicious applications loaded on the same MULTOS smart card as the Smart Folder 3 MULTOS application.

2.3.2. TOE Logical Boundary

The following Figure 3 defines the TOE Logical Boundary.

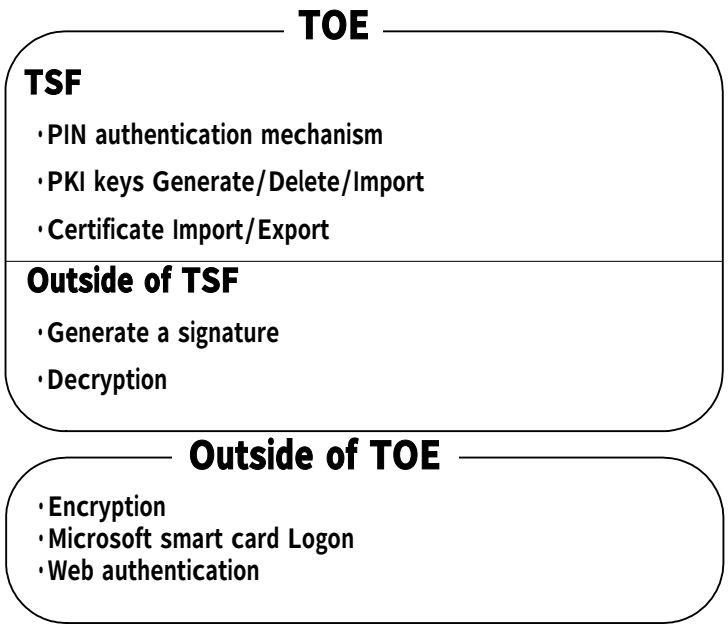

Figure 3 TOE Logical boundary

Figure 3 shows that the Smart Folder 3 product has two categories of functions: TOE functions and outside of TOE functions. The TOE functions are divided into TSP-enforcing and outside of TSF functions.

TSF includes PIN authentication function and PKI keys generate/delete/import.

- PIN authentication function guards the TOE.
- When PKI keys generate/delete/import, TOE holds the assets (PKI private key) safely.
- An authenticated user can import and export certificates.

Outside of TSF includes generate a signature, decryption. These are application functions of Smart Folder 3.

- An authenticated user can generate a signature on the TOE.
- An authenticated user can decrypt a data with the PKI private key.

Outside of TOE includes encryption, Microsoft Smartcard Logon and web authentication. Encryption means, for instance, the encryption of e-mails that is operated by e-mail software.

- Security software like e-mail software can encrypt a data with PKI public key.
- For Microsoft Smartcard Logon, refer to glossary terms.
- For web authentication, refer to glossary terms.

2.4. Objects

The TOE has following objects, which are used by each component to store data or save the TOE states. These are the assets of the TOE. The objects are:

1. Policy data

   The Policy data includes:

   A) Minimum length of normal user PIN

   B) Minimum length of administrator PIN

   C) Maximum number of consecutive wrong normal user PIN inputs

   D) Maximum number of consecutive wrong administrator PIN inputs

   E) Re-authentication flag for signing operation

   F) Re-authentication flag for decrypting operation

   An issuer defines the Policy data when issuing a card.

2. Card issue state flag

   This flag determines whether a card is issued or not. IssueState, which appears in this ST, is kept by this object.

3. PIN state flag

   This flag determines whether the Normal user PIN existing on a card is “Initial PIN” or not.

4. Normal user PIN (Normal user PIN length is included.)

5. Administrator PIN (Administrator PIN length is included.)

6. Wrong normal user PIN input counter

   This is for counting how many consecutive wrong normal user PIN inputs are attempted to a card. Exceeding the maximum number of consecutive wrong normal user PIN inputs results in a normal user PIN locked card. When Wrong normal user PIN input counter reaches Maximum number of consecutive wrong normal user PIN inputs, the TOE is normal user PIN locked and LockState is Normal User Lock. Administrator can unlock the Normal User Lock.

7. Wrong administrator PIN input counter

This is for counting how many consecutive wrong administrator PIN inputs are attempted to a card. Exceeding the maximum number of consecutive wrong administrator PIN inputs results in an administrator PIN locked card. When Wrong administrator PIN input counter reaches Maximum number of consecutive wrong administrator PIN inputs, the TOE is administrator PIN locked and LockState is Admin Lock.

8. PKI keys (private and public keys)

   A PKI key can be divided into two parts: one private key and one public key. A MULTOS smart card can hold two PKI keys (i.e. two pairs of a private key and a public key) at the maximum.

9. Digital certificates

   A MULTOS smart card can hold two certificates at the maximum. Certificates are stored using the FAT and the stored certificate data is managed using the certificate directory. A description on the FAT and the certificate directory is found in the Smart Folder 3 High Level Design Document.

10. Lock State

    Lock State holds the TOE lock state. The TOE lock state means if the TOE is administrator PIN locked, normal user PIN locked or not locked. Lock State has one of the following values.

    A) Admin Lock

       When one inputs wrong administrator PIN consecutively issuer-defined times, the TOE is administrator PIN locked and the Lock State is changed to Admin Lock. In this case, none can unlock the TOE so the TOE cannot be used anymore.

    B) Normal user Lock

       When one inputs wrong normal user PIN consecutively issuer-defined times, the TOE is normal user PIN locked and the Lock State is changed to Normal user Lock. In this case, administrator can unlock the TOE. After the unlocking, Lock State is changed to Not Lock.

    C) Not Lock

       The TOE is not locked. When the TOE is in this state, normal user can use the TOE for signing and decrypting operations.

Objects 11, 12 are session variables, which are stored in a volatile memory (i.e. the stored data will be cleared when a MULTOS smart card is taken out of a reader/writer).

11. Logon state

This will keep the Logon state of a card. It can have one of the following 5 values:

A) Log off

This means none is currently logging on a card.

B) Temporary log on

This means a user is currently logging on using an initial PIN, which is set by an issuer.

C) Log on

This means a user (either an administrator or a normal user) is currently logging on.

D) Issuing started

This means an issuer has started to issue a card. Only a new card (i.e. a card that has not been issued, yet) can have this value.

E) New card

This means a card has not been issued, yet.

The initializing routine mentioned above initializes this state according to the following rule:

- When the Card issue state flag is “not issued”, the Logon state will be “New card.”
- When the Card issue state flag is “issued”, the Logon state will be “Log off.”

The User type and this data are used for realizing the Smart Folder 3 Access Control Policy.

12. User type

This represents the type of a user, who is currently logging on a card. This will have one of two values: administrator or normal user. When none is logging on a card or after a card is pulled out of a reader/writer, this object is set to “normal user.”

The Logon state and this data are used for realizing the Smart Folder 3 Access Control Policy.

These objects are illustrated in Figure 4. They are divided into 2 categories: User Data and TSF Data.

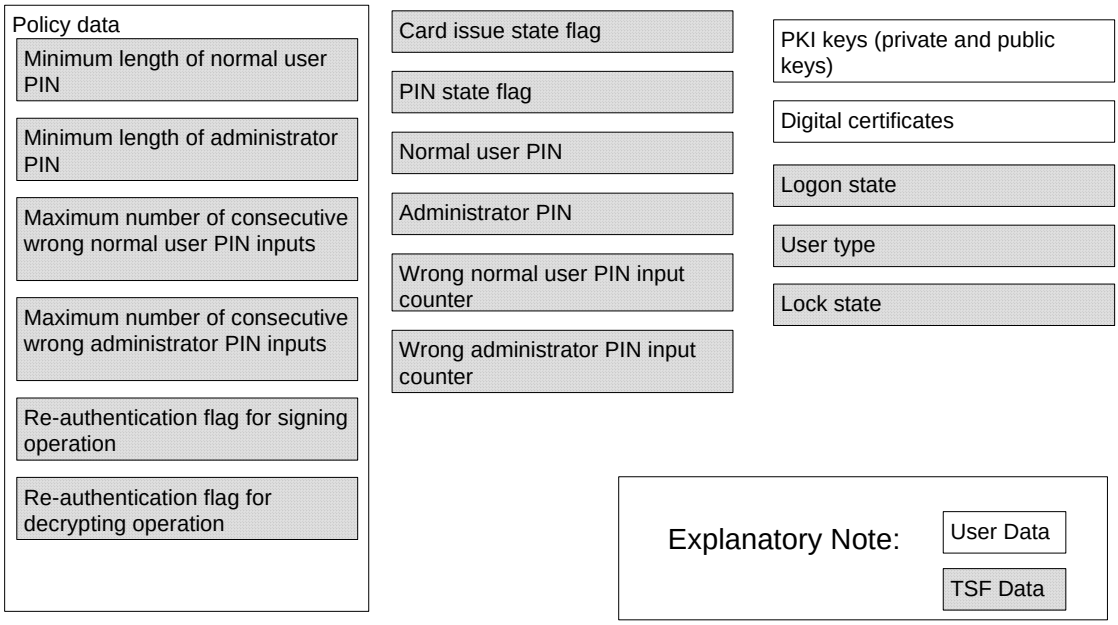

Figure 4 TOE Objects

2.5. Roles

There are 3 different roles for the Smart Folder 3. They are:

1. Issuer

   An issuer can set initial administrator and normal user PINs, store initial PKI keys, store Digital certificates and issue MULTOS smart card used by the Smart Folder 3. An issuer can define the Policy data, which is described at 2.4 Objects before issuing a MULTOS smart card.

2. Administrator

   An administrator can unlock normal user PIN locked MULTOS smart card and initialize MULTOS smart card when, for example, the MULTOS smart card owner retires.

3. Normal User

   A normal user can perform various operations including generating PKI keys and certificates, signing and decrypting.

The TOE distinguishes an administrator and a normal user by PIN authentication, and distinguishes issuer by the Logon state.

3. TOE Security Environment

This section describes:

1. Significant assumptions about the TOE's operational environment
2. Threats related to the TOE
3. Organizational Security Policy

3.1. Assumptions

The requirements listed below are supposed to be met by the environment under which the TOE operates. If these assumptions are not met, the TOE security cannot be maintained and the security to the assets is not guaranteed.

3.1.1. A.CARD

The TOE must run on MULTOS smart card. It is assumed that MULTOS chip implements countermeasures against hardware attacks (e.g. direct electrical modification or probing). The MULTOS OS also implements countermeasures against attacks from other applications loaded on a same MULTOS smart card by providing firewalls. Therefore MULTOS Smart card is safe.

3.1.2. A.ISSUER

It is assumed that issuer is not malicious and does what issuer is supposed to do correctly. The issuers set Minimum length of administrator PIN and Minimum length of normal user PIN of 6 characters or longer. The issuers must set the Re-authentication flag for signing operation and the Re-authentication flag for decrypting operation "enable". And the issuer must set the TOE lock function "ON".

3.1.3. A.ISSUERTOOL

It is assumed that only issuers can possess and use an issuer tool library. Only the issuer tool library can perform issuer operations. An attacker with low attack potential, which is expected for the TOE, can not develop a pseudo issuer tool library by guessing the TOE command and data structures.

3.1.4. A.PIN

It is assumed that users will keep their PIN secret and key inputs are not monitored by any means. And users select a PIN composed of at least one special character and one digit out of available special characters, digits and alphabets.

3.1.5. A.RW

It is assumed that the MULTOS smart card reader/writer used with the TOE works correctly and does not have any malicious functionality (e.g. stealing or modifying data going through it).

3.1.6. A.PC

It is assumed that the PC used with the TOE, operating system, other hardware, drivers and the cooperating PC software are properly managed and not infected with malicious codes or functionalities. Especially, cables connecting PC and peripherals must not be monitored.

3.1.7. A.IMPORTKEY

It is assumed that the TOE imports only not vulnerable PKI keys. The not vulnerable PKI keys can be utilized to generate a signature and/or decrypt encrypted information. And PKI private keys cannot be easily guessed from corresponding PKI public keys.

3.2. Threats

The TOE is required to counter threats. The threats are labeled with “T.”-started name.

The asset for the TOE is required for important transactions and for decrypting secret information. Attackers’ attack potential is supposed to be low. So, This ST defines attackers as those with attack potential of low.

3.2.1. T.ATTACK

An unauthorized person logs on the TOE. Then, the TOE is utilized to generate a signature and/or decrypt encrypted information by PKI private key.

3.2.2. T.GENKEY

An unauthorized person guesses PKI private key from PKI public key, when TOE generates vulnerable PKI keys.

3.2.3. T.SENDDATA

While normal user leaves the TOE without logging off after successful authentication, an unauthorized person uses PKI private key of the TOE.

3.2.4. T.IMPERSONATE

An unauthorized person tries the PIN-input thousands of times and eventually guesses the PIN, which is used for user authentication, and uses PKI private key of the TOE.

3.2.5. T.ATTACKTSFDATA

A malicious user modifies TSF data, to which an access is not permitted for the person, after logging on to the TOE.

3.2.6. T.ATTACKUSERDATA

A malicious user modifies User data, to which an access is not permitted for the person, after logging on to the TOE.

3.2.7. T.MODIFYPIN

A malicious user modifies the PIN stored in the TOE. And the malicious user illegally logs on.

3.2.8. T.RESIDUAL

A malicious user steals residual data after a deletion of secret data (e.g. the PKI private key) to restore the secret data.

3.2.9. T.ABUSE

If the TOE includes PKI private key, an unauthorized person abuses PKI private key of the TOE while the TOE is being delivered from an issuer’s site to a user’s site.

3.2.10. T.ADMIN

A malicious administrator of the TOE abuses a normal user’s PKI private key of the TOE.

3.3. Organizational Security Policies

There are no organizational security policies in this ST.

4. Security Objectives

Security objectives are categorized as below:

1. Security Objectives for the TOE
2. Security Objectives for the operational environment

The security objectives for the TOE are labeled with “O.”-started name. The security objectives for the operational environment are labeled with “OE.”-started name.

4.1. Security Objectives for the TOE

This section defines the security objectives for the TOE. These security objectives must be met to counter some of the threats identified in 3.2.

4.1.1. O.AUTHENTICATION

The TOE will ensure that an administrator and a normal user has been uniquely authenticated before sensitive operations such as signing and decrypting are possible. The number of authentication attempts is restricted (i.e. The range of Wrong normal user / administrator PIN input counter is within Maximum number of consecutive wrong normal user / administrator PIN inputs). After executing the authentication process, each command is called by the TSF if appropriate.

4.1.2. O.RESTRICTOPERATION

The TOE will ensure that the operations, which an administrator and a normal user can do, are restricted according to their User type (e.g. administrator or normal user). The TOE holds an administrator PIN and a normal user PIN to authenticate and distinguish administrator and normal user. The TOE distinguishes issuer by the fact that issuer has issuer tool library. Only normal user can perform sensitive operations (i.e. signing and decrypting operations). And administrator can unlock the normal user PIN locked TOE and/or initialize the TOE. Administrator can perform no operation that normal user can do. The TOE controls accesses to user data by authenticated users including only distinguished users.

4.1.3. O.USERCHECK

The TOE will ensure every time a user performs signing or decrypting operations that each user has been authenticated with PIN.

4.1.4. O.SECDATAPROTECTED

The TOE will ensure that Policy data cannot be modified after the MULTOS smart card is issued.

4.1.5. O.SECDATACONTROL

The TOE will ensure that the person with appropriate security role changes the security related data for authentication (i.e. Normal user/Administrator PIN and Wrong normal user PIN input counter) only when the change is requested by authenticated user who has appropriate role (e.g. administrator or normal user).

4.1.6. O.CLEARDATA

The TOE will ensure that all secret data is completely cleared at the timing of deletion and nobody can restore the information.

4.1.7. O.INITIALPIN

The TOE will ensure that when a user logs onto the TOE using the initial PIN, the user cannot access PKI private keys.

4.1.8. O.GENKEY

The TOE will provide a function to generate PKI keys that can be used for generating a signature and/or decrypting encrypted information and are not vulnerable.

4.2. Security Objectives for the Operational Environment

This section defines the security objectives for the operational environment. These security objectives must be met to realize assumptions for the operational environment identified in 3.1 and threats identifies in 3.2.

4.2.1. OE.CARD

TOE has to run on MULTOS smart card. The MULTOS smart card on which the TOE operates must prevent direct access to the information stored in it via hardware attacks. The MULTOS OS blocks attacks between a pair of two applications, which are loaded on the same MULTOS smart card, by providing firewalls between any pair of two applications. MULTOS smart card is purchased from the manufacturer that is trusted.

4.2.2. OE.SECRETPIN

The PIN shall be known to the owner only and shall not be disclosed to the others. A user must ensure that none is peeping his/her keyboard when inputting PIN. A user chooses a PIN that contains at least one special character and one digit out of available special characters, digits and alphabets.

4.2.3. OE.MANAGE

The PC, operating system and the PC software with which the TOE operates work correctly. The PC used with the TOE is managed and maintained to avoid a system failure. A user may prepare a duplicated system in case of emergency. A good vaccine program and the latest virus pattern file must be installed and activated. This is for protecting the PC from malicious codes. A user has to keep his/her PC in a safe environment to avoid attacks. Cables connected to the PC are occasionally checked to avoid information eavesdropping.

4.2.4. OE.ISSUER

The issuers are thoughtfully selected and trained not to abuse their tool. Only the issuer tool library can perform issuer operations. The issuers define the Minimum length of administrator PIN and the Minimum length of normal user PIN as 6 characters or longer. Issuer has to turn on the Re-authentication flag for signing operation and the Re-authentication flag for decrypting operation. And the issuer must set the TOE lock function “enable.”

4.2.5. OE.RW

Smart card Reader / Writer must be trustworthy.

4.2.6. OE.IMPORTKEY

A user must import only not vulnerable PKI keys to the TOE. The not vulnerable PKI keys can be utilized to generate a signature and/or decrypt encrypted information. And PKI private keys cannot be easily guessed from corresponding PKI public keys.

4.2.7. OE.INITIALPIN

A normal user must ensure that the initial PIN has not been changed while the TOE is delivered from an issuer's site to a normal user's site. And an issuer must define an initial PIN when issuing the MULTOS smart cards. An issuer must inform a normal user of the departure of the normal user's MULTOS smart card.

5. IT Security Requirements

5.1. TOE Security Requirements

This section describes the requirements that must be met by the TOE. The mark "*" of dependencies means the dependencies are not satisfied.

5.1.1. TOE Security Functional Requirements

The TOE contains a security function realized by a probabilistic or permutational mechanism. The function is PIN authentication for administrators and users. The minimum strength level claimed for this function is SOF-basic. So, the global minimum strength level claimed for the TOE will be SOF-basic.

FCS_CKM.1 uses a proprietary key generation algorithm but an analysis of strength of the algorithm is out of the scope of this evaluation. And there is no effect for SOF analysis.

5.1.1.1. FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: proprietary]** and specified cryptographic key sizes **[assignment: 1,024 bits]** that meet the following: **[assignment: none].**

Dependencies: *FCS_COP.1, FCS_CKM.4, *FMT_MSA.2

5.1.1.2. FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[assignment: zeroization]** that meets the following: **[assignment: FIPS 140-2, Section 4.7.6, Key Zeroization].**

Dependencies: FDP_ITC.1, *FMT_MSA.2

5.1.1.3. FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[assignment: User Data Access Control Policy]** on **[assignment:**
subject: processes related to normal user, administrator, issuer and Any ("Any" means subject is 'normal user' or 'administrator' or 'issuer'.)
object: PKI keys and Digital certificates
operation: Read, Write and Initialize
].

Dependencies: FDP_ACF.1

5.1.1.4. FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **[assignment: User Data Access Control Policy]** to objects based on **[assignment:**
States of the following TSF data:
IssueState (Issued or Not Issued),
LockState (Admin Lock, Normal User Lock or Not Lock) and
AuthState (New, ST Issue, Admin Logon, Normal User Logon, TEMP Logon and Logoff)
].

Note: AuthState is composed of Logon state and User type.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
[assignment: User Data Access Control Policy Rule defined in Table 1 **]**.

Table 1 User Data Access Control Policy Rule

User		Issuer		Any	Administrator	Any	Administrator	Normal User	Normal User	Any
IssueState		Not Issued		Issued						
LockState		Not Lock		Admin Lock	Normal User Lock		Not Lock			
AuthState		New	ST Issue	Logoff	Admin Logon	Logoff	Admin Logon	Normal User Logon	TEMP Logon	Logoff
PKI keys	PKI Private key	-	R/W	-	INIT	-	INIT	R/W	-	-
	PKI Public key	-	R/W	-		-		R/W	-	R
Digital certificates		-	R/W	-		-		R/W	-	R

Table 1 includes objects that are user data stored in a non-volatile memory. From the table, who (user) can read or write what (object) at what state can be known. The line "User" means who performs the operation. "IssueState" means the state Card issue state flag: "Issued" or "Not Issued." "LockState" means if a card is administrator PIN locked, normal user PIN locked or not locked. A card is administrator PIN locked when Wrong administrator PIN input counter exceeds Maximum number of consecutive wrong administrator PIN inputs. A card is normal user PIN locked when Wrong normal user PIN input counter exceeds Maximum number of consecutive wrong normal user PIN inputs. "AuthState" is determined by Logon state and User type, which are described in 2.4 Objects. How "AuthState" is determined is shown in Table 2

Table 2 AuthState Determination Table

AuthState	Logon state	User type
New	New card	-
ST Issue	Issuing started	-
Admin Logon	Log on	administrator
Normal User Logon	Log on	normal user
TEMP Logon	Temporary log on	normal user
Logoff	Log off	normal user

Lower half of the Table 1 shows what kind of operation can be performed to the objects. “R” means the user can read values from the object, “W” means the user can write values to the object and “R/W” means the user can read/write values from/to the object. “INIT” means the user can initialize the object (i.e. set the default value of the object and memory areas of PKI keys and digital certificates to character of zero). All objects are initialized simultaneously. “-“ means the user cannot access the object. For example, an administrator can read the Policy data but cannot write it.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[assignment: none]**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **[assignment: none]**.

Dependencies: FDP_ACC.1, *FMT_MSA.3

5.1.1.5. FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **[assignment: User Data Access Control Policy]** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC**: [assignment: none]**.

Dependencies: FDP_ACC.1, *FMT_MSA.3

5.1.1.6. FIA_AFL.1 Authentication failure handling

FIA_AFL.1:1 Administrator authentication failure handling

FIA_AFL.1.1:1 The TSF shall detect when **[assignment: issuer-defined number of consecutive]** unsuccessful authentication attempts occur related to **[assignment: the presentation of a wrong administrator PIN]**.

FIA_AFL.1.2:1 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment: deny any further operation (i.e. issuer, administrator or normal user cannot unlock)]**.

Dependencies: FIA_UAU.1

Note: Issuer-defined number of consecutive unsuccessful authentication attempts means Maximum number of consecutive wrong administrator PIN inputs.

FIA_AFL.1:2 Normal user authentication failure handling

FIA_AFL.1.1:2 The TSF shall detect when **[assignment: issuer-defined number of consecutive]** unsuccessful authentication attempts occur related to **[assignment: the presentation of a wrong normal user PIN]**.

FIA_AFL.1.2:2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **[assignment: deny any further operation except for administrator operations: unlocking a user PIN locked MULTOS smart card and/or initializing a MULTOS smart card]**.

Dependencies: FIA_UAU.1

Note: Issuer-defined number of consecutive unsuccessful authentication attempts means Maximum number of consecutive wrong normal user PIN inputs.

5.1.1.7. FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **[assignment: AuthState (administrator or normal user), Logon state (issuer)]**.

Dependencies: No Dependencies.

Note: Administrator and normal user are distinguished by the type of authentication commands (administrator logon or normal user logon) and authenticated by PIN. Administrator and normal user have separate PIN, respectively. Therefore administrator cannot log on to the TOE as normal user even if one inputs correct administrator PIN and vice versa. Issuer is distinguished by Logon state.

5.1.1.8. FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[assignment: Issuer-defined minimum length]**.

Note: the secrets mean the user and administrator PINs.

Dependencies: No Dependencies.

5.1.1.9. FIA_UAU.1 Timing of authentication

FIA_UAU.1 Allowed operation before authentication

FIA_UAU.1.1 The TSF shall allow **[assignment: reading Logon state, User type, Policy data, PKI public keys and Digital certificates]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 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

5.1.1.10. FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **[assignment: that a decrypting operation is required or that a signing operation is required]**.

Dependencies: No Dependencies.

5.1.1.11. FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to **[selection: disable, enable]** the functions **[assignment: re-authentication function and TOE lock function]** to **[assignment: the issuer]**.

Dependencies: FMT_SMR.1 (included in FMT_SMR.2)

Note: Disabling/enabling of re-authentication function means clearing/setting Re-authentication flag for signing / decrypting operation. Disabling/enabling of TOE lock function means setting Maximum number of consecutive wrong normal user/administrator PIN inputs.

5.1.1.12. FMT_MTD.1 Management of TSF data

FMT_MTD.1:1 Management of Normal user PIN

FMT_MTD.1.1: 1 The TSF shall restrict the ability to **[selection: modify]** the **[assignment: Normal user PIN]** to **[assignment: the normal user]**.

Dependencies: FMT_SMR.1 (included in FMT_SMR.2)

FMT_MTD.1:2 Management of Administrator PIN

FMT_MTD.1.1: 2 The TSF shall restrict the ability to **[selection: modify]** the **[assignment: Administrator PIN]** to **[assignment: the administrator]**.

Dependencies: FMT_SMR.1 (included in FMT_SMR.2)

FMT_MTD.1:3 Management of Wrong normal user PIN input counter

FMT_MTD.1.1: 3 The TSF shall restrict the ability to **[selection: clear]** the **[assignment: Wrong normal user PIN input counter]** to **[assignment: the administrator]**.

Dependencies: FMT_SMR.1 (included in FMT_SMR.2)

FMT_MTD.1:4 Management of Policy data

FMT_MTD.1.1: 4 The TSF shall restrict the ability to **[selection: modify]** the **[assignment: Policy data]** to **[assignment: the issuer]**.

Dependencies: FMT_SMR.1 (included in FMT_SMR.2)

FMT_MTD.1:5 Management of TSF data (Initialize)

FMT_MTD.1.1: 5 The TSF shall restrict the ability to **[selection: initialize]** the **[assignment: Policy data, Card issue state flag, PIN state flag, Normal user PIN (including Normal user PIN length), Administrator PIN (including Normal user PIN length), Wrong normal user PIN input counter, Wrong administrator PIN input counter]** to **[assignment: the administrator]**.

Dependencies: FMT_SMR.1 (included in FMT_SMR.2)

5.1.1.13. FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles **[assignment: issuer, administrator and normal user]**.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions **[assignment: None should be associated with more than one role]** are satisfied.

Dependencies: *FIA_UID.1

5.1.1.14. FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No Dependencies.

5.1.1.15. FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **[assignment: Normal user PIN, Administrator PIN]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use **[assignment: original PIN-related command parameter]** when interpreting the TSF data from another trusted IT product.

Dependencies: No Dependencies.

5.1.1.16. FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No Dependencies.

5.1.2. TOE Security Assurance Requirements

The assurance requirements for the TOE are constituted by evaluation assurance level EAL4.

5.2. Security Requirements for the IT Environment

There are no security requirements for the IT environment in this ST.

6. TOE Summary Specification

6.1. Access Control Policy

The Smart Folder 3 access control policy is shown in the Table 3:

TSF data and user data are included in this table. The mark “Y” in the TSF Data column means the corresponding data is TSF data and the mark “N” means the data is user data. The access control policy only for user data is picked out from the table and is called User Data Access Control Policy.

Table 3 Smart Folder 3 Access Control Policy

User	TSF Data	Issuer		Any	Administrator	Administrator	Any	Administrator	Administrator	Normal User	Normal User	Any
IssueState	Y	Not Issued		Issued								
LockState	Y	Not Lock		Admin Lock	Normal User Lock			Not Lock				
AuthState	Y	New	ST Issue	Logoff	Admin Logon		Logoff	Admin Logon		Normal User Logon	TEMP Logon	Logoff
Command	-	Any	Any	Any	Initialize	Other than Initialize	Any	Initialize	Other than Initialize	Any	Any	Any
Policy data	Y	-	R/W	R	INIT	R	R	INIT	R	R	R	R
Card issue state flag	Y	-	W	-		-	-		-	-	-	-
PIN state flag	Y	-	-	-		-	-		-	-	W	-
Normal user PIN (including Normal user PIN length)	Y	-	W	-		-	-		-	W	W	-
Administrator PIN (including Administrator PIN length)	Y	-	W	-		W	-		W	-	-	-
Wrong normal user PIN input counter	Y	-	-	-		CLEAR	-		CLEAR	-	-	-
Wrong administrator PIN input counter	Y	-	-	-		-	-		-	-	-	-
PKI keys PKI Private key	N	-	R/W	-		-	-		-	R/W	-	-
PKI keys PKI Public key	N	-	R/W	-		-	-		-	R/W	-	R
Digital certificates	N	-	R/W	-		-	-		-	R/W	-	R

Table 3 includes objects that are static variables stored in a non-volatile memory. From the table, who (user) can read or write what (object) at what state can be known. The line “User” means who performs the operation. “IssueState” means the state Card issue state flag: “Issued” or “Not Issued.” “LockState” means if a card is administrator PIN locked, normal user PIN locked or not locked. A card is administrator PIN locked when Wrong administrator PIN input counter exceeds Maximum number of

consecutive wrong administrator PIN inputs. A card is normal user PIN locked when Wrong normal user PIN input counter exceeds Maximum number of consecutive wrong normal user PIN inputs. “AuthState” is determined by Logon state and User type, which are described in 2.4 Objects. How “AuthState” is determined is shown in Table 4. And the line “Command” means what type of command an administrator performs. The cell in the line “Command”, which corresponds to TSF data, is “-“ because this line means command types, not data types. It is necessary because an administrator can “Initialize” a MULTOS smart card and at the time, he/she can initialize every object in the MULTOS smart card. “Any” in this line means any commands including “Initialize” and “Other than Initialize.”

Table 4 AuthState Determination Table

AuthState	Logon state	User type
New	New card	-
ST Issue	Issuing started	-
Admin Logon	Log on	administrator
Normal User Logon	Log on	normal user
TEMP Logon	Temporary log on	normal user
Logoff	Log off	normal user

Lower half of the Table 3 shows what kind of operation can be performed to the objects. “R” means the user can read values from the object, “W” means the user can write values to the object and “R/W” means the user can read/write values from/to the object. “INIT” means the user can initialize the object (i.e. set the default value of the object and memory areas of PKI keys and digital certificates to character of zero). All objects are initialized simultaneously. “CLEAR” means the user can reset the value of the object to 0. “-“ means the user cannot access the object. For example, an administrator can read the Policy data but cannot write it.

Default values of TSF data are shown in Table 5.

Table 5 Default values of TSF data

TSF data		Default value
Policy data	Minimum length of normal user PIN	6
	Minimum length of administrator PIN	6
	Maximum number of consecutive wrong normal user PIN inputs	6
	Maximum number of consecutive wrong administrator PIN inputs	6
	Re-authentication flag for signing operation	Disable
	Re-authentication flag for decrypting operation	Disable
Normal user PIN		A string of 32 “1”s.
Administrator PIN		A string of 32 “1”s.
Normal user PIN length		32
Administrator PIN length		32
Card issue state flag		Not Issued
PIN state flag		Initial PIN
Wrong normal user PIN input counter		0
Wrong administrator PIN input counter		0

Note that a PKI key includes a PKI private key and a PKI public key. And PKI private keys cannot be read out by any means. The mark, “R” for the PKI public key and Digital Certificate indicates that only the public portion of the PKI keys can be read. And version number of the TOE can be retrieved at any time though it is not stored in the TOE as an object.

Description about each object follows:

1. Policy data

   Policy data can only be set by an issuer when a card is not issued. An issuer must first start issuing a MULTOS smart card by changing Logon state from “New card” to “Issuing started” before writing the Policy data. After a card is issued, anyone can read the Policy data but none can modify it.

2. Card issue state flag

   This flag shows if a card is issued or not. So only issuer can change the value from “not issued” to “issued.” An issuer must first start issuing a MULTOS smart card by changing Logon state from “New card” to “Issuing started” before issuing a MULTOS smart card. After a card is issued, none can change the value back to “not issued.” There is only one case when the value can be changed from “issued” to “not issued.” It is when an administrator initializes the card.

3. PIN state flag

   This flag represents the state of normal user PIN and can have two values: temporary and permanent. If the PIN state is temporary, normal user can log on to the card and can only change normal user PIN. Once the normal user change the initial PIN, this flag changes to permanent and the normal user can perform

normal user operations including signing and decrypting. So only the normal user can change the value from “Initial PIN” to “permanent PIN” when he/she logs on to a card as “Temporary log on.” When a card is initialized by an administrator, the value changes back to “Initial PIN.”

4. Normal user PIN

   As already mentioned above, the normal user PIN is initially set by an issuer and gave to a normal user. The normal user changes his/her PIN periodically when he/she logs on to a MULTOS smart card. None can read the PIN from a card.

5. Administrator PIN

   The Administrator PIN is initially set by an issuer. When an administrator performs administrator operations, he/she must show the Administrator PIN. He/she can also change the PIN when he/she logs on to a MULTOS smart card as an administrator. None can read the PIN from a card.

6. Wrong normal user PIN input counter

   This is a counter used by the TSF to count the number of consecutive wrong normal user PIN input attempts. None can read the value from a card. When the value exceeds the limit, which is Maximum number of consecutive wrong normal user PIN inputs defined in the Policy data, the card is locked and denies normal user operations subsequently. An administrator can reset the counter to zero to unlock a locked card. A normal user has an opportunity to recover his/her locked card because losing precious information stored in a card can sometimes cause serious bad effects (e.g. the normal user may no longer read encrypted data).

7. Wrong administrator PIN input counter

   This is a counter used by the TSF to count the number of consecutive wrong administrator PIN input attempts. None can read the value from a card. When the value exceeds the limit, which is Maximum number of consecutive wrong administrator PIN inputs defined in the Policy data, the card is locked and denies any further operations except reading Policy data.

8. PKI keys

   A PKI key includes a PKI private key and a PKI public key. A normal user can read (i.e. performing signing or decrypting operations) or write (i.e. generating or importing PKI keys) the PKI keys. In addition, by the necessity, an issuer can store PKI keys in a card before a card is issued. Anyone (e.g. Microsoft smart card logon) can read the PKI public key, when User is Any, IssueState is Issued, LockState is NotLock and AuthState is Logoff.

9. Digital certificates

   A card can store Digital certificates corresponding to PKI keys stored on the card. A normal user can read or write (i.e. importing certificate data) the certificate data. In addition, an issuer can store initial certificates in a card before a card is issued. Anyone (e.g. Microsoft smart card logon) can read the Digital certificates,

when User is Any, IssueState is Issued, LockState is NotLock and AuthState is Logoff.

6.2. TOE Security Functions

This section describes security functions provided by the TOE to meet the SFRs specified for the Smart Folder 3 MULTOS application in this ST.

Each security function is labeled with “SF.”-started name.

6.2.1. SF.ACCESSCONTROL

The TOE enforces User Data Access Control Policy for all accesses to PKI keys and Digital certificates. Accesses to these objects are allowed/denied by IssueState (Issued or Not Issued), LockState (Admin Lock, Normal User Lock or Not Lock) and AuthState (New, ST Issue, Admin Logon, Normal User Logon, TEMP Logon and Logoff) following User Data Access Control Policy.

The TOE refuses unauthorized subject to access TSF data and TSF.

Authentication function is called firstly every time a user uses the TOE. Other functions are called by the authentication function. Therefore, none can bypass the authentication function.

6.2.2. SF.CARDLOCK

Issuer can set maximum number of consecutive wrong normal user PIN inputs and maximum number of consecutive wrong administrator PIN inputs before issuing the MULTOS smart card and can disable/enable TOE lock function.

If wrong PINs are inputted consecutively (i.e. every time a correct PIN is presented, Wrong normal user PIN input counter and Wrong administrator PIN input counter are cleared) for issuer-defined times, the MULTOS smart card is locked. When the MULTOS smart card is locked by a normal user PIN, administrator can log on to the MULTOS smart card and do whatever operation he/she can do when the MULTOS smart card is not locked (including clearing Wrong normal user PIN input counter). When the MULTOS smart card is locked by an Administrator PIN, the MULTOS smart card cannot be used anymore.

This Policy data can never be changed after the MULTOS smart card issuance. So, the once-determined Policy data cannot be modified unless the MULTOS smart card is initialized by the administrator.

6.2.3. SF.INITIALIZE

The TOE allows an administrator to initialize Policy data, Card issue state flag, PIN state flag, Normal user PIN (including Normal user PIN length), Administrator PIN (including Normal user PIN length), Wrong normal user PIN input counter and Wrong administrator PIN input counter. The default values for this initialization are shown in Table 5. The TOE refuses to initialize TSF data separately.

The TOE refuses unauthorized subject to access TSF data and TSF.

6.2.4. SF.PINAUTHENTICATION

The TOE distinguishes a user as one of the following roles: issuer, administrator or normal user. A user cannot have two roles from issuer, administrator and normal user, simultaneously. Issuer is distinguished by Logon state. When Logon state is Issuing started, the TOE distinguishes the user as an issuer. Administrator and normal user are distinguished by AuthState as defined in Table 4 AuthState Determination Table. To change the AuthState, a user must be distinguished and authenticated. Administrator and normal user are distinguished by the type of authentication commands (administrator logon or normal user logon) and authenticated by PIN. Administrator and normal user have separate PIN, respectively. Therefore administrator cannot log on to the TOE as normal user even if one inputs correct administrator PIN and vice versa.

Issuer uses the TOE only before the MULTOS smart card is issued. The TOE only distinguishes issuer. Issuer is distinguished by Logon state, and can do allowed operations to the TOE. When administrator and normal user uses the TOE after the MULTOS smart card is issued by an issuer, administrator and normal user are authenticated, and can do allowed operations to the TOE. Logon state, User type, Policy data, PKI public keys and Digital certificates can be read out from the TOE by anyone without Authentication. This is because these data is required by the Microsoft smart card logon before a user is authenticated.

The PIN information is interpreted accordingly by the TOE and by the cooperating PC software following the original PIN-related command parameter. The command for PIN change has a parameter that is used for distinguishing which of the two types of PIN (i.e. Administrator PIN or Normal user PIN) is going to be exchanged.

When a PIN is to be changed, the TOE requires a presentation of the correct current PIN (in fact, it is the message digest). None can change the PIN without knowing the current PIN.

The normal user PIN and the administrator PIN must be at least issuer-defined characters long. For each PIN, the maximum length is 32. PIN may be composed of alphanumeric characters and special characters (!”#$%&’()~=|-^@[;:],./¥`{+*}<>?_).

If the new PIN does not match the PIN-length Policy data, the PIN change attempt is rejected.

A normal user and an administrator can modify the normal user PIN and the Administrator PIN, respectively. None other can modify these PINs.

The normal user PIN defined by an issuer is called the “Initial PIN” and when a user logs onto the TOE using the initial PIN, the user cannot access PKI private keys.

The PIN authentication is realized by a probabilistic or permutational mechanism. The strength of function claimed for this function is SOF-basic.

6.2.5. SF.PINLENGTHMANAGE

Issuer can set Minimum length of administrator / normal user PIN before issuing the MULTOS smart card. After the MULTOS smart card is issued these values cannot be changed.

When administrator / normal user tries to change one's PIN and inputs new PIN shorter than Minimum length of administrator / normal user PIN, the TOE denies the change of PIN.

6.2.6. SF.PRIVATEKEY

PKI keys are generated using the proprietary cryptographic key generation algorithm and have key length of 1,024 bits.

When PKI keys are deleted, the TOE removes the PKI keys in non-volatile memory completely following the FIPS 140-2, Section 4.7.6 Key Zeroization.

Import of PKI private keys and Digital certificates are controlled by User Data Access Control Policy.

6.2.7. SF.REAUTH

The TOE has a re-authentication function. When MULTOS smart card are issued, issuers can set Policy data for each MULTOS smart card. This Policy data includes re-authentication flag for signing and decrypting operations. Issuer can decide and set up so that authentication must be done every time before operation is done. This Policy data is set for the signing and decrypting operations.

If an issuer does not set the Policy data, the flags are "disable" as a default.

This Policy data can never be changed after the MULTOS smart card issuance. So, the once-determined Policy data cannot be modified unless the MULTOS smart card is initialized by the administrator.

6.3. Relations to Functional Requirements Rationale

Relations between the TOE Security Functions and the TOE Security Functional Requirements are shown at 8.3 TOE Summary Specification Rationale.

For relations between all security functions and security functional requirements, refer to Table 6.

Table 6 Security Functional Requirements and Summary Specification Rationale

	SF.ACCESSCONTROL	SF.CARDLOCK	SF.INITIALIZE	SF.PINAUTHENTICATION	SF.PINLENGTHMANAGE	SF.PRIVATEKEY	SF.REAUTH
FCS_CKM.1						X	
FCS_CKM.4						X	
FDP_ACC.1	X						
FDP_ACF.1	X						
FDP_ITC.1						X	
FIA_AFL.1:1		X					
FIA_AFL.1:2		X					
FIA_ATD.1				X			
FIA_SOS.1				X			
FIA_UAU.1				X			
FIA_UAU.6							X
FMT_MOF.1		X					X
FMT_MTD.1:1				X			
FMT_MTD.1:2				X			
FMT_MTD.1:3		X					
FMT_MTD.1:4		X			X		X
FMT_MTD.1:5			X				
FMT_SMR.2				X			
FPT_RVM.1	X						
FPT_TDC.1				X			
FPT_SEP.1	X		X				

6.4. Assurance Measures

This section shows the assurance measures for the TOE. Nineteen documents, the source code of the TOE and the TOE itself are included. They are:

1. Smart Folder 3 Configuration Management
2. Visual Source Safe 6.0 Intruction Manual
3. Development Member List
4. Configuration List
5. Smart Folder 3 Life Cycle Management
6. TOE Managing List
7. Smart Folder 3 life-cycle definition

8. Smart Folder 3 Security Policy Model
9. Smart Folder 3 Functional Specification
10. Smart Folder 3 High-level Design
11. Smart Folder 3 Low-level Design
12. Smart Folder 3 Delivery Procedures
13. Smart Folder 3 Instruction Manual for Smart Folder 3 Issuer Tool Library
14. Smart Folder 3 Instruction Manual for Smart Folder 3 Administrator Tool
15. Smart Folder 3 Instruction Manual for Smart Folder 3 User Tool
16. Smart Folder 3 Test Documentation
17. Smart Folder 3 Vulnerability Analysis
18. Smart Folder 3 Correspondence Analysis
19. Smart Folder 3 Security Target
20. Smart Folder 3 Source Code
21. Smart Folder 3 (the TOE)

For relations between these assurance measures and assurance requirements, refer to Table 7.

Table 7 Assurance Measures Rationale

Assurance class	Assurance requirement component(s)	Assurance measure(s)
ASE: Security Target Evaluation	ASE_DES.1, ASE_ENV.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1, ASE_SRE.1, ASE_TSS.1, ASE_PPC.1	*Smart Folder 3 Security Target*
ACM: Configuration Management	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2	*Smart Folder 3 Configuration Management* *Visual Source Safe 6.0Intruction Manual* *Development Member List* *Configuration List*
ADO: Delivery and Operation	ADO_DEL.2	*Smart Folder 3 Delivery Procedures*
	ADO_IGS.1	*Smart Folder 3 Instruction Manual for Smart Folder 3 Issuer Tool Library* *Smart Folder 3 Instruction Manual for Smart Folder 3 Administrator Tool* *Smart Folder 3 Instruction Manual for Smart Folder 3 User Tool*
ADV: Development	ADV_FSP.2	*Smart Folder 3 Functional Specification*
	ADV_HLD.2	*Smart Folder 3 High-level Design*
	ADV_IMP.1	*Smart Folder 3 Source Code*
	ADV_LLD.1	*Smart Folder 3 Low-level Design*
	ADV_RCR.1	*Smart Folder 3 Correspondence Analysis*
	ADV_SPM.1	*Smart Folder 3 Security Policy Model*
AGD: Guidance Documents	AGD_ADM.1,	*Smart Folder 3 Instruction Manual for Smart Folder 3 Issuer Tool Library* *Smart Folder 3 Instruction Manual for Smart Folder 3 Administrator Tool*
	AGD_USR.1	*Smart Folder 3 Instruction Manual for Smart Folder 3 User Tool*
ALC: Life Cycle Support	ALC_DVS.1, ALC_LCD.1, ALC_TAT.1	*Smart Folder 3 Life Cycle Management* *TOE Managing List* *Smart Folder 3 life-cycle definition*
ATE: Tests	ATE_COV.2, ATE_DPT.1, ATE_FUN.1	*Smart Folder 3 Test Documentation*
	ATE_IND.2	*Smart Folder 3 MULTOS Application* (the TOE) *Smart Folder 3 Test Documentation*
AVA: Vulnerability Assessment	AVA_MSU.2, AVA_SOF.1, AVA_VLA.2	*Smart Folder 3 Vulnerability Analysis*

7. PP Claims

There is no PP referenced by this ST.

8. Rationale

8.1. Security Objectives Rationale

As for the following Table 8, security object and environment are coped with threat, organizational security policy and assumption. The place where X is shown threat/assumption copes with security object/environment.

Table 8 Security Objectives Rationale

	O.AUTHENTICATION	O.RESTRICTOPERATION	O.USERCHECK	O.SECDATAPROTECTED	O.SECDATACONTROL	O.CLEARDATA	O.INITIALPIN	O.GENKEY	OE.CARD	OE.SECRETPIN	OE.MANAGE	OE.ISSUER	OE.RW	OE.IMPORTKEY	OE.INITIALPIN
T.ATTACK	X	X													
T.GENKEY								X							
T.SENDDATA			X												
T.IMPERSONATE	X	X													
T.ATTACKTSFDATA				X											
T.ATTACKUSERDATA		X													
T.MODIFYPIN	X				X										
T.RESIDUAL						X									
T.ABUSE							X								X
T.ADMIN		X													
A.CARD									X						
A.ISSUER												X			
A.ISSUERTOOL												X			
A.PIN										X					
A.RW													X		
A.PC											X				
A.IMPORTKEY														X	

T.ATTACK is covered by O.AUTHENTICATION and O.RESTRICTOPERATION because normal user has to be authenticated before sensitive operations are performed (The TOE distinguishes issuer by the fact that issuer has issuer tool library.), and only the normal user can perform sensitive operations. The issuer and administrator cannot perform these operations.

T.SENDDATA is covered by O.USERCHECK because normal user is required to be authenticated every time before executing signing and decrypting operations.

T.IMPERSONATE is covered by O.AUTHENTICATION and O.RESTRICTOPERATION because normal user and administrator have to be authenticated and distinguished before sensitive operations are performed (The TOE distinguishes issuer by the fact that issuer has issuer tool library). And the number of consecutive wrong normal user / administrator PIN inputs are restricted to Maximum number of consecutive wrong normal user / administrator PIN inputs or less.

T.ATTACKTSFDATA is covered by O.SECDATAPROTECTED because TSF data cannot be modified after the MULTOS smart card is issued.

T.ATTACKUSERDATA is covered by O.RESTRICTOPERATION because an authenticated and distinguished user, including only distinguished user, can access the user data, to which the access is permitted according to the user's role.

T.GENKEY is covered by O.GENKEY because TOE generates PKI keys that can be used for generating a signature and/or decrypting encrypted information and are not vulnerable.

T.MODIFYPIN is covered by O.AUTHENTICATION and O.SECDATACONTROL because the PIN can be changed only when the change is requested by authenticated user who has appropriate role (e.g. administrator or normal user). One has to log on prior to the PIN change.

T.RESIDUAL is covered by O.CLEARDATA because the PKI private key is completely cleared at the timing of deletion and none can restore the PKI private key.

T.ABUSE is covered by O.INITIALPIN and OE.INITIALPIN because an issuer defines an initial PIN when issuing MULTOS smart cards. And a user cannot access PKI private keys by logging onto the TOE using an initial PIN. A normal user can detect an abuse of the MULTOS smart card under the following conditions:
1. A MULTOS smart card does not arrive though a MULTOS smart card departure notice has been arrived from an issuer.

2. An initial PIN has been changed when a normal user receives a MULTOS smart card.

T.ADMIN is covered by O.RESTRICTOPERATION because the TOE does not allow the administrator to perform normal user sensitive operations.

A.CARD is covered by OE.CARD because the TOE runs on MULTOS smart card. The MULTOS smart card prevents direct memory access and attack to the stored information. MULTOS smart card is purchased from the manufacturer that is trusted.

A.ISSUER is covered by OE.ISSUER because the issuers are trusted people who are trained not to abuse their privileges and they do their job correctly. They are supposed to issue MULTOS smart card with the Minimum length of administrator PIN and the Minimum length of normal user PIN of 6 characters or longer. And Issuer has to enable re-authentication function and TOE lock function.

A.ISSUERTOOL is covered by OE.ISSUER because only issuers can obtain the issuer tool library. Only the issuer tool library can perform issuer operations.

A.PIN is covered by OE.SECRETPIN because only the user shall know the PIN and the user shall not tell the PIN to anyone else. And key inputs are not monitored so they are not peeped over user's shoulder. Every PIN shall contain at least one special character and one digit.

A.RW is covered by OE.RW because smart card Reader / Writer is trustworthy.

A.PC is covered by OE.MANAGE because the PC, operating system and the PC software with which the TOE operates are maintained to work correctly. A good vaccine program and the latest virus pattern file must be installed and activated. A user has to keep his/her PC in a safe environment to avoid attacks. Especially, cables are maintained to avoid information eavesdropping.

A.IMPORTKEY is covered by OE.IMPORTKEY because the TOE imports only not vulnerable PKI keys. The not vulnerable PKI keys can be utilized to generate a signature and/or decrypt encrypted information. And PKI private keys cannot be easily guessed from corresponding PKI public keys.

8.2. Security Requirements Rationale

8.2.1. Appropriateness of the TOE Assurance Requirements

The PKI private key needs high level of security. If someone steals the PKI private key, he/she can pretend to be the original PKI private key owner. He/she can sign an important document like company contract, or can decrypt and read confidential information. This can be a serious threat to the original owner. So the TOE seems to require thorough testing and evaluation to ensure that the TOE can protect PKI private keys from attackers with low attack potential. However, the cost needed for the evaluation cannot be ignored. Therefore EAL4 seems to be appropriate. This level is said to be the highest level for commercial products and the TOE will be analyzed in detail.

8.2.2. Appropriateness of the Strength of Function

The asset protected by the TOE is used for important transactions and for decrypting secret information. Attackers are supposed to be with attack potential of low, as described in 3.1.7. This is because the possibility of attacks by those with high attack potential is low. Therefore, the TOE has the strength of SOF-basic.

8.2.3. Fulfillment of the TOE Objectives by the TOE Functional Requirements

As for the following Table 9, security object is coped by TOE functional requirements. The place where it is shown with X means security object copes with functional requirements.

Table 9 TOE Objectives and TOE Functional Requirements Rationale

	FCS_CKM.1	FCS_CKM.4	FDP_ACC.1	FDP_ACF.1	FDP_ITC.1	FIA_AFL.1:1	FIA_AFL.1:2	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.6
O.AUTHENTICATION						X	X	X	X	X	
O.RESTRICTOPERATION			X	X	X						
O.USERCHECK											X
O.SECDATAPROTECTED											
O.SECDATACONTROL											
O.CLEARDATA		X									
O.INITIALPIN			X	X							
O.GENKEY	X										

	FMT_MOF.1	FMT_MTD.1:1	FMT_MTD.1:2	FMT_MTD.1:3	FMT_MTD.1:4	FMT_MTD.1:5	FMT_SMR.2	FPT_RVM.1	FPT_TDC.1	FPT_SEP.1
O.AUTHENTICATION									X	
O.RESTRICTOPERATION						X	X	X		X
O.USERCHECK										
O.SECDATAPROTECTED	X				X					
O.SECDATACONTROL		X	X	X			X			
O.CLEARDATA										
O.INITIALPIN										
O.GENKEY										

O.AUTHENTICATION is met by FIA_UAU.1 and FIA_ATD.1. These functional requirements ensure that only Policy data and some other can be extracted from the TOE before successful authentication. After a user is authenticated and distinguished

as a normal user, he/she can perform signing and decrypting operations. Two roles, administrator and normal user, are defined and the TOE uses them for access control.

O.AUTHENTICATION is also met by following supportive components.

- FIA_AFL.1:1, FIA_AFL.1:2: This component limits the number of PIN input attempts. This will prevent an attacker from trying huge number of random PIN inputs and eventually guessing the correct PIN. Thus, this strengthens the authentication functions.
- FIA_SOS.1: This component limits the minimum length of administrator PIN and the minimum length of normal user PIN. This will prevent an attacker from trying huge number of random PIN inputs and eventually guessing the correct PIN.
- FPT_TDC.1: This component ensures that the TOE and the cooperating PC software can understand PIN data each other. There is a rule how to represent the data between them.

O.RESTRICTOPERATION is met by FMT_MTD.1:5, FDP_ACC.1, FDP_ACF.1, FDP_ITC.1, FMT_SMR.2, FPT_RVM.1 and FPT_SEP.1. These functional requirements ensure that there are three types of people concerning a system containing the TOE. These are issuer, administrator and normal user. These users will be distinguished accordingly by the TOE. And user operations are controlled by User Data Access Control Policy. The TOE refuses unauthorized subject to access TSF data and TSF. The authentication functions are activated first when the TOE starts running. This can prevent a bypassing of the authentication function, which is the TSF.

O.USERCHECK is met by FIA_UAU.6. This functional requirement ensures that each user must be authenticated every time before signing and decrypting operations even if the user has been authenticated once before.

O.SECDATAPROTECTED is met by FMT_MOF.1 and FMT_MTD.1:4. These functional requirements ensure that only issuer can change the Re-authentication flag for signing operation and the Re-authentication flag for decrypting operation, the Maximum number of consecutive wrong normal user PIN inputs and the Maximum number of consecutive wrong administrator PIN inputs and Minimum length of administrator PINs and Minimum length of normal user PINs. These changes can only be made before MULTOS smart card is issued. After MULTOS smart card is issued, only authorized user can modify appropriate TSF data. This will prevent an attack like disabling limit and try to figure out a correct PIN by attempting as many times of PIN input as the attacker wants to do.

O.SECDATACONTROL is met by FMT_MTD.1:1, FMT_MTD.1:2 , FMT_MTD.1:3 and FMT_SMR.2. These functional requirements ensure that only a normal user can change his/her own normal user PIN anytime he/she wants to, and only an

administrator can change his/her Administrator PIN or clear Wrong normal user PIN input counter. (i.e. unlock a normal user PIN locked MULTOS smart card.)

O.CLEARDATA is met by FCS_CKM.4. This functional requirement ensures that sensitive information like PKI private key will be cleared completely at the timing of deletion. This is realized by writing zero onto the memory where the data was on.

O.INITIALPIN is met by FDP_ACC.1 and FDP_ACF.1. These functional requirements ensure that when a user logs onto the TOE using the initial PIN, the user cannot access PKI private keys.

O.GENKEY is met by FCS_CKM.1. This functional requirement ensures that PKI keys are generated using a proprietary PKI key generation algorithm.

8.2.4. Dependencies Rationale

Dependencies among functional requirement components are satisfied as shown in Table 10. The mark "*" means the dependencies are not satisfied.

Table 10 Functional Requirement Components Dependencies

Functional Requirement Components	Dependent to
FCS_CKM.1	*FCS_COP.1, FCS_CKM.4, *FMT_MSA.2
FCS_CKM.4	FDP_ITC.1, *FMT_MSA.2
FDP_ACC.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 *FMT_MSA.3
FDP_ITC.1	FDP_ACC.1, *FMT_MSA.3
FIA_AFL.1:1	FIA_UAU.1
FIA_AFL.1:2	FIA_UAU.1
FIA_ATD.1	Nothing
FIA_SOS.1	Nothing
FIA_UAU.1	*FIA_UID.1
FIA_UAU.6	Nothing
FMT_MOF.1	FMT_SMR. 1 (included in FMT_SMR.2)
FMT_MTD.1:1	FMT_SMR. 1 (included in FMT_SMR.2)

Functional Requirement Components	Dependent to
FMT_MTD.1:2	FMT_SMR. 1 (included in FMT_SMR.2)
FMT_MTD.1:3	FMT_SMR. 1 (included in FMT_SMR.2)
FMT_MTD.1:4	FMT_SMR. 1 (included in FMT_SMR.2)
FMT_MTD.1:5	FMT_SMR. 1 (included in FMT_SMR.2)
FMT_SMR.2	*FIA_UID.1
FPT_RVM.1	Nothing
FPT_TDC.1	Nothing
FPT_SEP.1	Nothing

Rationales for not covering dependencies are shown below:

FCS_CKM.1 depends on FCS_COP.1 but the FCS_COP.1 is not included in this ST. Because cryptographic operations are conducted by MULTOS OS (i.e. the cryptographic operations are conducted outside of the TOE).

FCS_CKM.1 and FCS_CKM.4 depend on FMT_MSA.2 but FMT_MSA.2 is not included in this ST because PKI keys do not have any security attributes.

FDP_ACF.1 and FDP_ITC.1 depend on FMT_MSA.3 but FMT_MSA.3 is not included in this ST because the TOE does not have security attributes for objects so there is no need for initialization of security attributes when objects are generated or imported.

FIA_UAU.1 depends on FIA_UID.1 but FIA_UID is not included in this ST because the TOE relates a user type to each distinguished role.

FMT_SMR.2 depends on FIA_UID.1 but FIA_UID.1 is not included in this ST because the TOE uses a function that distinguishes the user type instead of FIA_UID.1.

8.2.5. Mutual Support of Security Requirements Claim

As shown in 8.2.4 the functional security requirements, excluding some exceptions, form a mutually supportive whole.

There is no explicit dependency other than the functional requirements shown in 8.2.4, the explanations below show some rationale regarding implicit dependencies among them.

FPT_RVM.1 prevents bypassing of all of the TOE security functional requirements.

FPT_SEP.1 prevents unauthorized subject to access to TSF or TSF data. FMT_MOF.1 prevents de-activation of the re-authentication function and TOE lock function by a person other than an issuer because only an issuer can enable/disable re-authentication function and TOE lock function.

8.2.6. Fulfillment of the IT Environment Objectives by the IT Environment Functional Requirements

There is no fulfillment of the IT environment objectives by the IT environment functional requirements in this ST.

8.3. TOE Summary Specification Rationale

8.3.1. Security Functions Rationale

Table 6 shows which security functional requirements cover which security functions. There is no additional information in IT security functions. So no potential security vulnerability is introduced to the TOE.

Table 11 gives descriptions about relations between security functional requirements and TOE security functions.

Table 11 Security Functional Requirements and Summary Specification Rationale Description

Functional requirement	Summary Specification
FCS_CKM.1	SF.PRIVATEKEY: "PKI keys are generated using the proprietary cryptographic key generation algorithm and have key length of 1,024 bits." This means PKI keys are generated using the intended algorithm and have intended key length.
FCS_CKM.4	SF.PRIVATEKEY: "When PKI keys are deleted, the TOE removes the PKI keys in non-volatile memory completely following the FIPS 140-2, Section 4.7.6 Key Zeroization." This means the TOE clears the memory area where a PKI private key exists when a normal user deletes the PKI private key.
FDP_ACC.1, FDP_ACF.1	SF.ACCESSCONTROL: "The TOE enforces User Data Access Control Policy for all accesses to PKI keys and Digital certificates without exception. Accesses to these objects are allowed/denied by IssueState (Issued or Not Issued), LockState (Admin Lock, Normal User Lock or Not Lock) and AuthState (New, ST Issue, Admin Logon, Normal User Logon, TEMP Logon and Logoff) following User Data Access Control Policy." This means there is a restriction on what can be done by either an issuer, an administrator or a normal user.
FDP_ITC.1	SF.PRIVATEKEY: "Import of PKI private keys and Digital certificates are controlled by User Data Access Control Policy." This means imports of PKI private keys and Digital certificates are controlled by User Data Access Control Policy.

Functional requirement	Summary Specification
FIA_AFL.1:1 FIA_AFL.1:2	SF.CARDLOCK: "If wrong PINs are inputted consecutively (i.e. every time a correct PIN is presented, Wrong normal user PIN input counter and Wrong administrator PIN input counter are cleared) for issuer-defined times, the MULTOS smart card is locked. When the MULTOS smart card is locked by a normal user PIN, administrator can log on to the MULTOS smart card and do whatever operation he/she can do when the MULTOS smart card is not locked (including clearing Wrong normal user PIN input counter). When the MULTOS smart card is locked by an Administrator PIN, the MULTOS smart card cannot be used anymore." This means the MULTOS smart card is locked after a consecutive certain number of wrong PIN inputs. When a MULTOS smart card is locked by the Administrator PIN, the MULTOS smart card will deny any further request. When a MULTOS smart card is locked by the normal user PIN, an administrator can unlock the MULTOS smart card.
FIA_ATD.1	SF.PINAUTHENTICATION: "The TOE distinguishes a user as one of the following roles: issuer, administrator or normal user. A user cannot have two roles from issuer, administrator and normal user, simultaneously. Issuer is distinguished by Logon state. When Logon state is Issuing started, the TOE distinguishes the user as an issuer. Administrator and normal user are distinguished by AuthState as defined in Table 4 AuthState Determination Table. To change the AuthState, a user must be distinguished and authenticated. Administrator and normal user are distinguished by the type of authentication commands (administrator logon or normal user logon) and authenticated by PIN. Administrator and normal user have separate PIN, respectively. Therefore administrator cannot log on to the TOE as normal user even if one inputs correct administrator PIN and vice versa. Issuer uses the TOE only before the MULTOS smart card is issued. The TOE only distinguishes issuer. Issuer is distinguished by Logon state, and can do allowed operations to the TOE. When administrator and normal user uses the TOE after the MULTOS smart card is issued by an issuer, administrator and normal user are authenticated, and can do allowed operations to the TOE. Logon state, User type, Policy data, PKI public keys and Digital certificates can be read out from the TOE by anyone without Authentication. This is because these data is required by the Microsoft smart card logon before a user is authenticated." These functions mean a user is distinguished by the TOE as issuer, administrator or normal user.
FIA_SOS.1	SF.PINAUTHENTICATION: "The normal user PIN and the administrator PIN must be at least issuer-defined characters long." This means every PIN, for both an administrator and a normal user, has the length of at least the issuer-defined characters.

Functional requirement	Summary Specification
FIA_UAU.1,	SF.PINAUTHENTICATION: "The TOE distinguishes a user as one of the following roles: issuer, administrator or normal user. A user cannot have two roles from issuer, administrator and normal user, simultaneously. Issuer is distinguished by Logon state. When Logon state is Issuing started, the TOE distinguishes the user as an issuer. Administrator and normal user are distinguished by AuthState as defined in Table 4 AuthState Determination Table. To change the AuthState, a user must be authenticated. Administrator and normal user are distinguished by the type of authentication commands (administrator logon or normal user logon) and authenticated by PIN. Administrator and normal user have separate PIN, respectively. Therefore administrator cannot log on to the TOE as normal user even if one inputs correct administrator PIN and vice versa. Issuer uses the TOE only before the MULTOS smart card is issued. The TOE only distinguishes issuer. Administrator and normal user uses the TOE after the MULTOS smart card is issued by an issuer and are authenticated. Only after a user is authenticated as an issuer, an administrator or a normal user, one can do allowed operations to the TOE. Logon state, User type, Policy data, PKI public keys and Digital certificates can be read out from the TOE by anyone without Authentication. This is because these data is required by the Microsoft smart card logon before a user is authenticated. The normal user PIN distinguished by an issuer is called the "Initial PIN" and when a user logs onto the TOE using the initial PIN, the user cannot access PKI private keys." This means one has to be authenticated as either an administrator or a normal user before operating the TOE after the MULTOS smart card is issued. Anyone can read Logon state、User type, Policy data, PKI public keys and Digital certificates. When a user logs onto the TOE using the initial PIN, the user cannot access PKI private keys. Administrator and normal user are distinguished by the type of authentication commands (administrator logon or normal user logon) and authenticated by PIN.
FIA_UAU.6	SF.REAUTH: "The TOE has a re-authentication function. When MULTOS smart card are issued, issuers can set Policy data for each MULTOS smart card. This Policy data includes re-authentication flag for signing and decrypting operations. Issuer can decide and set up so that authentication must be done every time before operation is done. This Policy data is set for the signing and decrypting operations." This means a user is re-authenticated before signing or decrypting operations if the flag is set. There are two flags and these are for signing and decrypting, respectively.
FMT_MOF.1	SF.CARDLOCK: "Issuer can set maximum number of consecutive wrong normal user PIN

Functional requirement	Summary Specification
	inputs and maximum number of consecutive wrong administrator PIN inputs before issuing the MULTOS smart card and can disable/enable TOE lock function." This means only issuers can disable/enable TOE lock function.
FMT_MOF.1	SF.REAUTH: "When MULTOS smart card are issued, issuers can set Policy data for each MULTOS smart card. This Policy data includes re-authentication flag for signing and decrypting operations. Issuer can decide and set up so that authentication must be done every time before operation is done. This Policy data is set for the signing and decrypting operations." This means only issuers can determine the Policy data about re-authentication.
FMT_MTD.1:1 FMT_MTD.1:2	SF.PINAUTHENTICATION: "When a PIN is to be changed, the TOE requires a presentation of the correct current PIN (in fact, it is the message digest). None can change the PIN without knowing the current PIN." These functions mean an administrator and a normal user can change their PIN, respectively when they present the correct current PIN.
FMT_MTD.1:3	SF.CARDLOCK: "When the MULTOS smart card is locked by a normal user PIN, administrator can log on to the MULTOS smart card and do whatever operation he/she can do when the MULTOS smart card is not locked (including clearing Wrong normal user PIN input counter)." This function means unlocking a normal user PIN locked MULTOS smart card (i.e. clearing the Wrong normal user PIN input counter) is performed only by an administrator.
FMT_MTD.1:4	SF.CARDLOCK: "Issuer can set maximum number of consecutive wrong normal user PIN inputs and maximum number of consecutive wrong administrator PIN inputs before issuing the MULTOS smart card." This function means an issuer can modify maximum number of consecutive wrong normal user PIN inputs and maximum number of consecutive wrong administrator PIN input, which are included in Policy data.
FMT_MTD.1:4	SF.PINLENGTHMANAGE: "Issuer can set Minimum length of administrator / normal user PIN before issuing the MULTOS smart card. After the MULTOS smart card is issued these values cannot be changed. This function means an issuer can modify Minimum length of administrator / normal user PIN, which is included in Policy data.

Functional requirement	Summary Specification
FMT_MTD.1:4	SF.REAUTH: "When MULTOS smart card are issued, issuers can set Policy data for each MULTOS smart card. This Policy data includes re-authentication flag for signing and decrypting operations. Issuer can decide and set up so that authentication must be done every time before operation is done. This Policy data is set for the signing and decrypting operations." These functions mean only issuers can set a Policy data for re-authentication flag for signing and decrypting operations.
FMT_MTD.1:5	SF.INITIALIZE: "TOE allows an administrator to initialize Policy data, Card issue state flag, PIN state flag, Normal user PIN (including Normal user PIN length), Administrator PIN (including Normal user PIN length), Wrong normal user PIN input counter and Wrong administrator PIN input counter. The default values for this initialization are shown in Table 5." This means an administrator can initialize the TOE.

Functional requirement	Summary Specification
FMT_SMR.2	SF.PINAUTHENTICATION: "The TOE distinguishes a user as one of the following roles: issuer, administrator or normal user. A user cannot have two roles from issuer, administrator and normal user, simultaneously. Issuer is distinguished by Logon state. When Logon state is Issuing started, the TOE distinguishes the user as an issuer. Administrator and normal user are distinguished by AuthState as defined in Table 4 AuthState Determination Table. To change the AuthState, a user must be distinguished and authenticated. Administrator and normal user are distinguished by the type of authentication commands (administrator logon or normal user logon) and authenticated by PIN. Administrator and normal user have separate PIN, respectively. Therefore administrator cannot log on to the TOE as normal user even if one inputs correct administrator PIN and vice versa. Issuer uses the TOE only before the MULTOS smart card is issued. The TOE only distinguishes issuer. Issuer is distinguished by Logon state, and can do allowed operations to the TOE. When administrator and normal user uses the TOE after the MULTOS smart card is issued by an issuer, administrator and normal user are authenticated, and can do allowed operations to the TOE. Logon state, User type, Policy data, PKI public keys and Digital certificates can be read out from the TOE by anyone without Authentication. This is because these data is required by the Microsoft smart card logon before a user is authenticated." This means these three roles: issuer, administrator and normal user, have completely different capability and responsibility. The Smart Folder 3 is distributed as one of the three components: issuer tool library, administrator tool and user tool. And every user uses one of them. The TOE distinguishes User type by parameters (e.g. logon command has a parameter that is used to specify the command is for administrator or normal user). The issuer tool library is available only to issuers. The administrator tool and user tool are used by anyone including malicious people and this is not a threat to the TOE. Because a user is authenticated on the TOE and not on the tools. And none can have two roles simultaneously.
FPT_RVM.1	SF.ACCESSCONTROL: "Authentication function is called firstly every time a user uses the TOE. Other functions are called by the authentication function. Therefore, none can bypass the authentication function." This means the TOE can distinguish a user before other functions can be operated. This prevents unauthorized person from using the TOE without being authenticated.

Functional requirement	Summary Specification
FPT_TDC.1	SF.PINAUTHENTICATION: "The PIN information is interpreted accordingly by the TOE and by the cooperating PC software following the original PIN-related command parameter. The command for PIN change has a parameter that is used for distinguishing which of the two types of PIN (i.e. Administrator PIN or Normal user PIN) is going to be exchanged." This function means the TOE can read and use the PIN, which is inputted at a cooperating PC, for authentication of the user and changing PIN.
FPT_SEP.1	SF.ACCESSCONTROL: "The TOE enforces User Data Access Control Policy for all accesses to PKI keys and Digital certificates. Accesses to these objects are allowed/denied by IssueState (Issued or Not Issued), LockState (Admin Lock, Normal User Lock or Not Lock) and AuthState (New, ST Issue, Admin Logon, Normal User Logon, TEMP Logon and Logoff) following User Data Access Control Policy. The TOE refuses unauthorized subject to access TSF data and TSF." This function means TSF data and TSF are protected from tampering of unauthorized subjects.
FPT_SEP.1	SF.INITIALIZE: "TOE allows an administrator to initialize Policy data, Card issue state flag, PIN state flag, Normal user PIN (including Normal user PIN length), Administrator PIN (including Normal user PIN length), Wrong normal user PIN input counter and Wrong administrator PIN input counter. The default values for this initialization are shown in Table 5. The TOE refuses unauthorized subject to access TSF data and TSF." This function means TSF data and TSF are protected from tampering of unauthorized subjects.

FMT_MTD.1:4 is covered by SF.CARDLOCK, SF.PINLENGTHMANAGE and SF.REAUTH independently (i.e. not by the combination of SF.CARDLOCK, SF.PINLENGTHMANAGE and SF.REAUTH).

FMT_MOF.1 is covered by SF.CARDLOCK and SF.REAUTH independently (i.e. not by the combination of SF.CARDLOCK and SF.REAUTH).

FPT_SEP.1 is covered by SF.ACCESSCONTROL and SF.INITIALIZE independently (i.e. not by the combination of SF.ACCESSCONTROL and SF.INITIALIZE).

8.3.2. Strength of Security Functions Consistency Rationale

Only probabilistic or permutational security function in the TOE is SF.PINAUTHENTICATION. The SF.PINAUTHENTICATION has the strength of SOF-basic as described in 6.2.4. The minimum strength of function for the TOE is claimed to be SOF-basic in 5.1.1. These two strength of functions are both SOF-basic and, without further explanation, are apparently consistent.

8.3.3. Assurance Measures Rationale

The Table 7 lists all assurance requirements from the assurance level of EAL4 and the ASE class, which is for this ST itself evaluation.

8.4. PP Claims Rationale

There is no PP referenced by this ST.