Application

GemVision Smart D/C

masquée sur le composant

ST19SF08AC

(Référence ST19SF08AC/RMY)

TABLE OF CONTENTS

1. ST INTRODUCTION

1.1 ST identification

Title: " GemVision Smart D/C" Security Target.

Version: 1.5

French IT Security Evaluation and Certification Scheme (SCSSI):.....

This ST has been built with CC Version 2.1.

The software reference and versions of this ST are described in section 11.

1.2 ST overview

The aim of this document is to describe the Security Target (ST) of the "GemVision Smart D/C " product .

The product is a Gemplus software embedded (ES) on a Smartcard Integrated Circuit.

The main objectives of this ST are:

- to describe the Target-Of-Evaluation (TOE) as a banking card for a Debit/Credit application.
- to define the limits of the TOE .
- to describe the security requirements for the TOE.

This application is based on the Smartcard Integrated Circuit to perform payment or cash withdraw transaction. This application has been launched to improve security provided by the Smartcard IC and its embedded software compliant to both EMV standard (EuroPay-MasterCard-Visa) and VIS (Visa Integrated Circuit Specification).

1.2.1 THE TOE ACTORS

The debit/credit banking application involves several actors :

1.2.1.1 Payment organization

The payment organization is a company which members are banks; the aim of this organization is to ensure inter-operability among banks worldwide. For this product, VISA is the payment organization.

VISA :

- defines and controls inter-operability rules.
- operates the communication network and process transaction clearing.
- is responsible for specification, quality, security and functionality of the relevant technology (cards, terminals, servers and communication systems) that take part of the Debit/Credit application.

1.2.1.2 Card issuer

The card issuer -short named " issuer "- is a bank. The bank issues cards to its customers that are the " Card-Holders ". The card belongs to the card issuer. Therefore the card issuer is responsible for :

- personalization.
- distribution.
- invalidation.

The PIN management is the responsibility of both Issuer and Card-Holder.

1.2.1.3 The product developer

The developer design the chip ES. The product developer is Gemplus.

1.2.1.4 The silicon manufacturer

The silicon manufacturer -or founder- designs, manufactures and load the ES in the Smartcard IC.

1.2.1.5 The card manufacturer

The card manufacturer is responsible for manufacturing Smartcards. For this product, the card manufacturer is Gemplus.

1.2.1.6 The personalizer

The personalizer personalizes the card by loading the card issuer and Card-Holder data as well as application secrets such as cryptographic keys and PIN.

1.2.1.7 The Card-Holder

The Card-Holder is a customer of the Card-Issuer. The card is personalized with the Card-Holder identification and secrets.

1.2.1.8 The Service-Provider

It is the merchant or any organization that provide services.

1.2.1.9 The Service-Provider Bank

The Service Provider-Bank is the Bank that receives the transaction amount for the service provided (cash withdrawal, face-to-face purchase, vending/ticketing machine, internet purchase). The Service-Provider Bank may paid by the acquirer.

1.2.2 THE TOE USERS

The " users " of the card are the Card-Holder, the -Bank, terminals like Automatic Teller Machine (ATM), Point-Of-Sales terminal (POS), vending machines as well as the card issuer.

1.2.3 THE TOE ADMINISTRATORS

The " administrators " of the card are the Card-Manufacturer, the Personalizer, the Card-Issuer.

1.2.4 THE LIMITS OF THE TOE

Phase	Limit of the TOE	Industrial Step	Industrial Step Deliverables	Logical Phase	TOE main administrator	TOE users	Construction	PP 9806	PP 9810
1	Construction	Design	Software		Product Developer		Gemplus		X
2	Construction	Design	Hard mask set		Silicon Manufacturer		ST	X	
3	Construction	Production	Wafers with Chips.	Chip Initialization	Silicon Manufacturer		ST	X	
4	Usage	Production	Modules		Card Manufacturer	Module Manufacturing Process			
5	Usage	Production	Card with embedded module.	Card Initialization	Card Manufacturer	Card Initialization system and process			
6	Usage	Personalization	Card personalized	Card Personalization	Card Personalizer	Card Personalization system and process			
7	Usage	Application (End Usage)			Card-Issuer	Card-Holder, Service Provider Card Issuer Terminals			

Table 1-1 : Limits of the TOE

The limits of the TOE are taken from §2.2 of the PP9810: As defined in the PP9810, "the limits of the TOE correspond to phase 1, including the software and corresponding data delivery to the IC manufacturer, and to the embedded software working on the IC as delivered by the IC manufacturer at the end of phase 3.

Phase 2 correspond to the IC development phase which is not part of the TOE. As required in PP/9810, the IC development objectives will be covered by the use of an IC which meets PP/9806.

The limits are marked in white in this table and the rest of the life cycle of the product is marked grey.

The operating system is a "closed " operating system. The software is compiled from both "C " language and Assembler language. It is not a " Open " operating system were the code is interpreted during execution.

The operating system does not support operating system extension during usage phases i.e. phases 4,5,6,7.

1.2.5 THE AIM OF THE DEBIT/CREDIT APPLICATION

The TOE is aimed to fight the following risks.

1.2.5.1 Transaction repudiation

A fraudulent card holder may deny a legal transaction .

1.2.5.2 Risk management by-pass

This issue covers risks relevant to fraudulent usage the card by the card-holder. It is a transaction forced illegally to off-line authorization when the card risk management should have normally required an on-line authorization.

1.2.5.3 Disabled card usage

This risk occurs when a end-user (legal or not) is using a card that has been deactivated.

1.2.5.4 Transaction corruption

An fraudulent Service-Provider may try to increase a legal transaction amount.

1.2.5.5 Transaction creation

An fraudulent Service-Provider may try to create an illegal transaction.

1.2.5.6 Illegal duplication of a card

A fraudulent organization may try to issue illegal cards.

1.2.5.7 Logical simulation of a card

When transactions scheme are not “ face-to-face ” (ATM, e-commerce, vending machines) fraudulent actors may try to emulate the logical behaviour of a genuine card.

1.2.6 CONTRIBUTION OF THE TOE IN THE APPLICATION

- Transaction signature.
- Authentication of the card holder.
- Authentication of the TOE other users.
- Authentication of the TOE administrators.
- Risk management based decision process.
- Confidentiality of cryptographic keys, PIN, ES.
- Integrity of cryptographic keys, PIN, ES, protected data.
- External communication protection against disclosure and corruption (secure messaging).
- Data files protected by access conditions driven by the ES.

1.3 CC conformance claim

This ST is compliant with the Common Criteria V2.1, parts 1,2,3.

This ST is inspired fromthe Protection Profile PP/9810 Version 1.2 dated November 19th ‘98 registered at the French Certification Body SCSSI. Nevertheless due to the assurance level (EAL4) it is not compliant with the PP9810

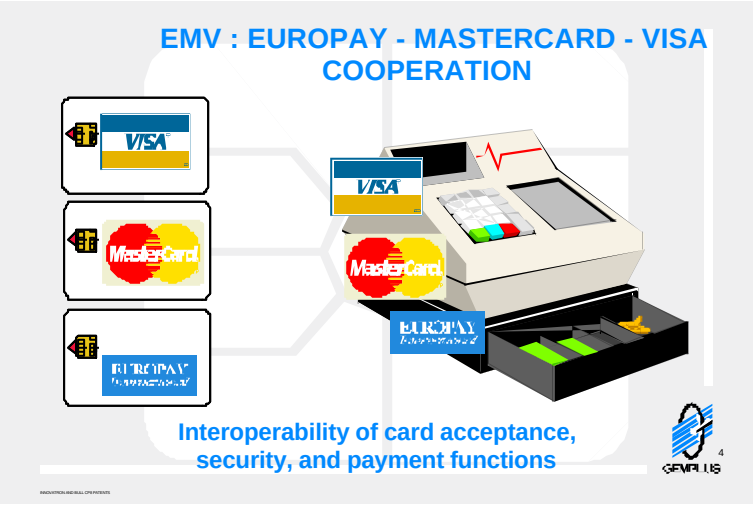
The Assurance level is EAL4 augmented; the minimum strength level for the TOE security functions is SOF-high for all the TOE security functions.

2. TOE DESCRIPTION

2.1 Product type

Smart Debit/Credit is a banking smartcard ES (Embedded Software) based on the Europay-Mastercard-Visa specification, EMV (also known as VME)‘96 Integrated Circuit Card Specification for Payment Systems, release 3.1.1, May 31 1998.

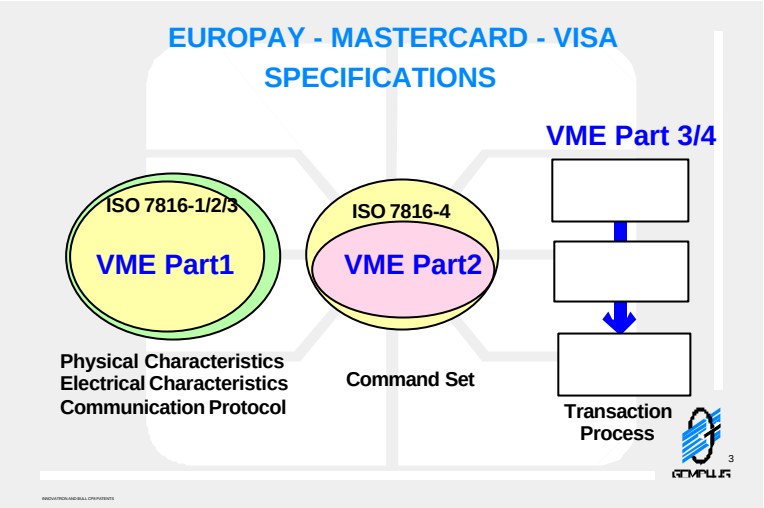
This de facto standard is aimed to insure interoperability between “ credit cards ” with embedded chips and credit-card-application such as Point Of Sales (POS), Automated Teller Machines (ATM).



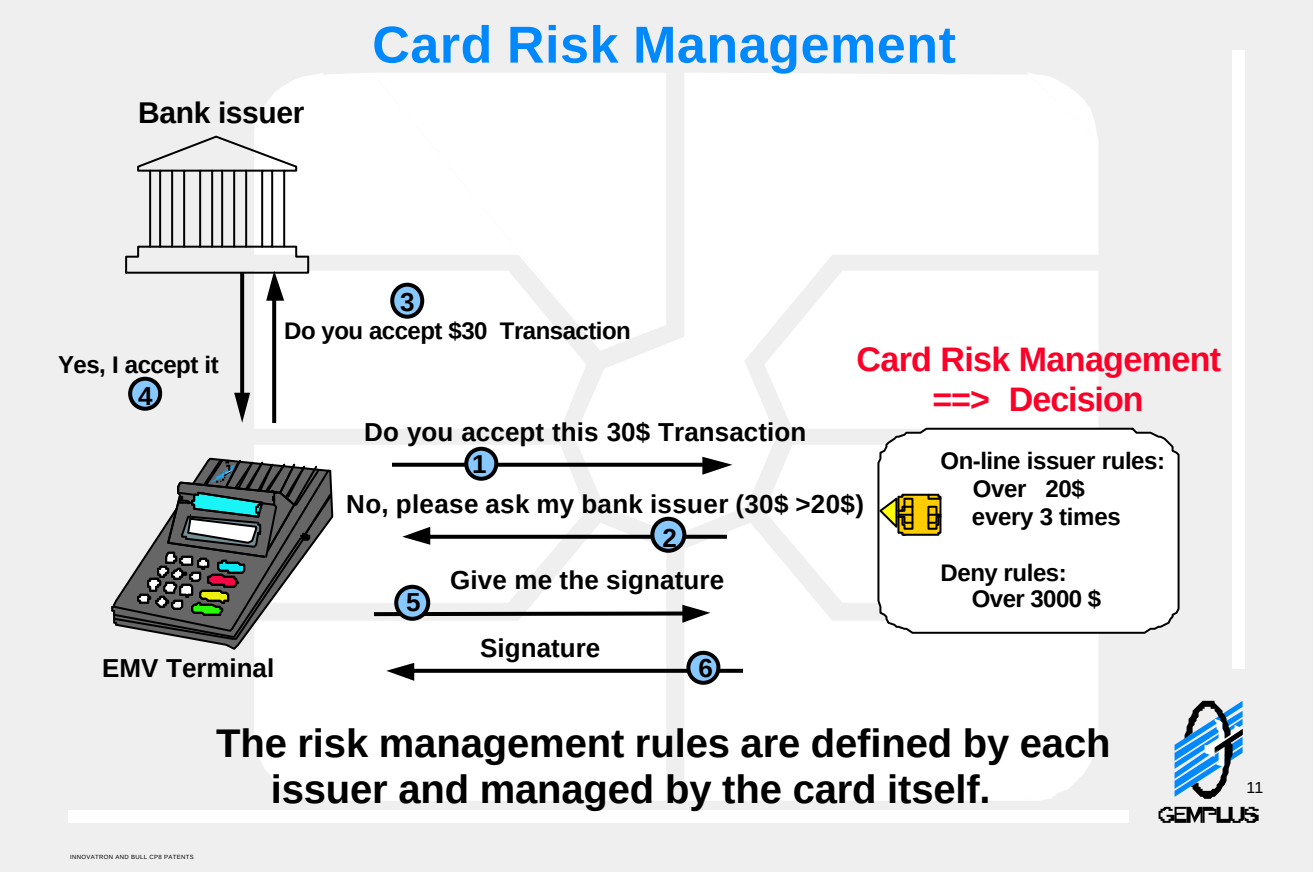
The system will avoid every “ credit card ” transaction to require a on-line telephone connection to save transaction time as well as telecom charges.

Decision on transaction (accepted off-line, accepted on-line, refused) is made by the 3 parts of the application system that are : Server, Terminal, Card. Both terminal and card have a risk management capability.

The example of such a nationwide application is the French Carte Bleue where the cost of fraud has been significantly dropped thanks to the release of chip card technology in the credit cards transactions. This is why the world-wide major payment associations Europay-Mastercard-Visa have created this international standard. UK is the first country that will launch credit cards compatible with this standard.



EMV is based on ISO 7816 standards.



Card Risk Management.

When a transaction is processed, then

0) the card is inserted in the terminal after the purchase amount has been inserted by the merchant in the terminal.

1) the terminal ask the card for risk decision (OK off-line, go on-line, refused)

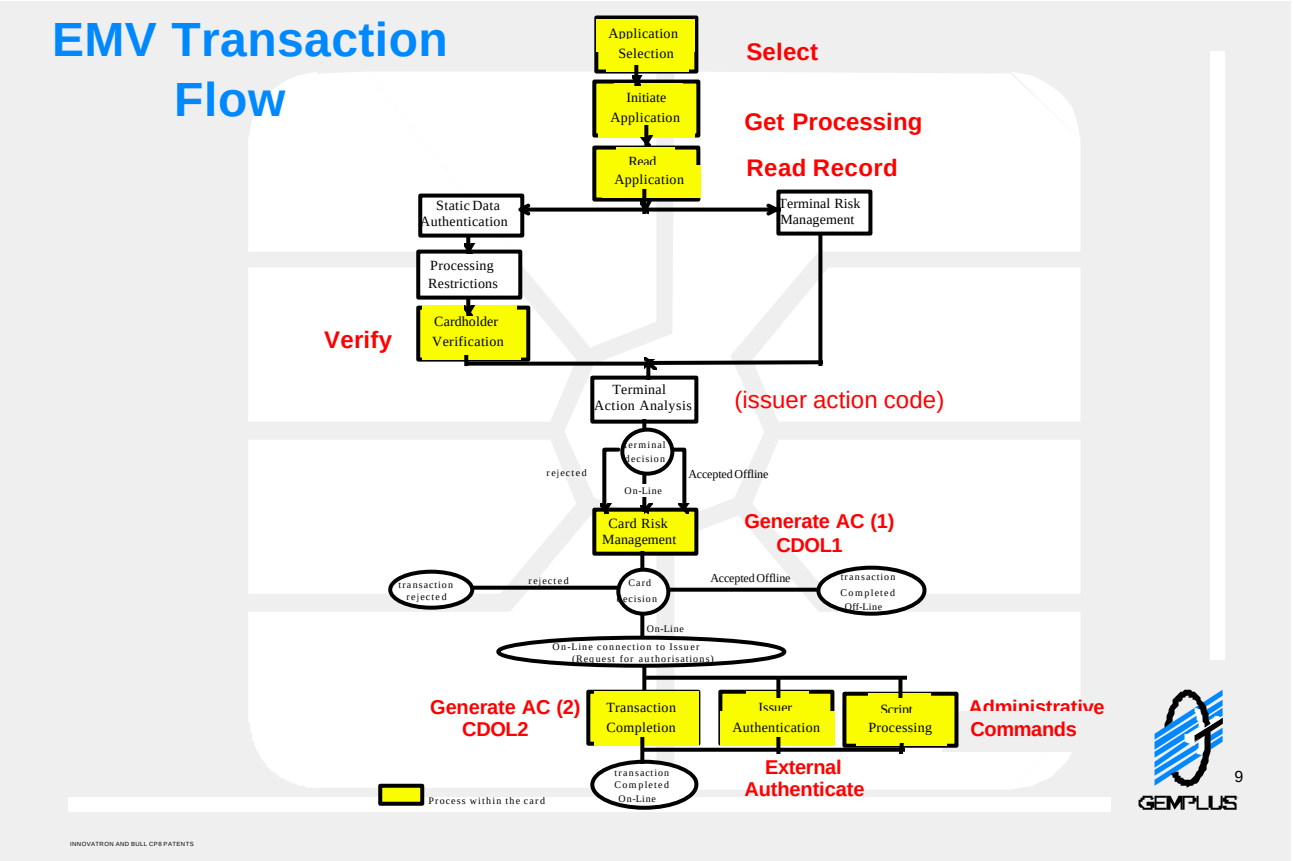
2) when card ask for on-line:

3) terminal will ask the bank server the payment OK.

4) the bank server will answer the payment OK

5) the terminal will then ask the ask for signature.

6) the card will sign the payment with a certificate.



Here is the card transaction flow based on risk management.

Extract from the VISA VIS specification overview for clarification purpose:

" When a card is presented to a terminal, the terminal determines which applications are supported by both the card and terminal. If the Smart Debit/Credit application is selected, the terminal requests that the card indicates the data to be used for that application. The terminal reads that data from the card and determines whether to perform off-line data authentication. Off-line data authentication is used to ensure that the card data has not been fraudulently altered since the card was personalised

If off-line data authentication is to be performed, the terminal uses the card data read from the card along with the application's 'signature', which is created from signing the card data with the private key of the RSA public key algorithm. The terminal verifies the signed card- and Card-Holder-related data using the Issuer's public key (which is stored in the card signed by the Visa private key) and the Visa public key (which is stored in the terminal) and compares it to the clear data to ensure that they match.

The terminal determines if the Card-Holder should be prompted to enter a Card-Holder Verification Method (CVM) based upon the issuer's CVM data initialised in the card. Card-Holder verification is used to ensure that the Card-Holder is legitimate and the card is not lost or stolen. If the card supports an off-line personal identification number (PIN) and terminal supports an offline PIN pad, the terminal may prompt the Card-Holder to enter the PIN and transmits the plaintext PIN to the card, which matches it against the PIN stored in the card to ensure that they match.

Both the terminal and card may perform off-line risk management (for example, floor limit checking, transaction velocity checking) to determine whether the transaction should be approved, declined, or transmitted on-line for authorisation. If both the card and the terminal indicate that the transaction satisfied the criteria for off-line authorisation, the transaction can be approved offline, and the card generates a DES-based cryptogram called the transaction certificate (TC) based on card-, transaction-, and terminal-related data. The TC and the data used to generate it are transmitted in the clearing message for future Card-Holder disputes and/or chargeback purposes. A TC may be used as a 'proof' of transaction when a Card-Holder incorrectly repudiates a transaction or to verify that the transaction data has not been changed by the merchant or acquirer. A cryptogram identical to the TC is generated for a declined transaction.

If the criteria for off-line authorisation are not satisfied, the terminal transmits an on-line request message to the issuer (or its agent) indicating why the transaction was transmitted on-line (if the terminal has on-line capability). Prior to the transaction being transmitted online, the card generates a cryptogram called the Authorisation Request Cryptogram (ARQC) based on card-, transaction-, and terminal-related data. The terminal transmits the ARQC and the data used to generate it in the request message. During on-line processing, the issuer performs card authentication to verify that the transmitted ARQC is valid (in other words, to ensure that the card data has not been skimmed from a genuine card to a counterfeit card). The issuer generates a reference ARQC using the clear data transmitted in the request message and compares it to the transmitted ARQC to ensure that they match.

The issuer then may use the ARQC to create a second cryptogram called the Authorisation Response Cryptogram, which is sent to the card in the response message and is used by the card to verify that the issuer is genuine. Issuer authentication is used to ensure that certain security-related parameters in the card are not reset after an on-line authorisation unless the issuer is proven to be genuine. This prevents criminals from circumventing the card's security features by simulating on-line processing and fraudulently 'approving' a transaction. If the issuer authentication fails, the card cannot be used to generate further off-line transactions. Issuer authentication is performed using a method similar to that used for card authentication.

The issuer may choose to transmit certain commands in the response message, which the terminal transmits to the card to perform functions such as updating card parameters, blocking the application, unblocking the offline PIN, etc. This is called Issuer Script processing.

To successfully complete the transaction, the card generates a TC as described above. If the terminal transmits a clearing message subsequent to an authorisation message, the TC is transmitted in the clearing message. If the terminal transmits a single message to the acquirer, the terminal may not transmit a separate message containing the TC to the acquirer. "

The card risk management is based upon the set of rules defined in the VIS specification and the parameters set by the issuer during personalization, and possibly updated by an authorized administrator during the applicative phase of the product life (phase 7). These parameters are stored as Application Proprietary TLV Objects in the TOE.

2.2 Smart card product life cycle

See PP/9810 and Table 1-1 : Limits of the TOE.

2.3 TOE environment

See PP/9810.

2.4 TOE logical phases

See PP/9810 and Table 1-1 : Limits of the TOE.

3. TOE SECURITY ENVIRONMENT

3.1 Threats

- The aim of the debit/credit application as well as the contribution of the TOE have been explained in the ST overview.
- The limits of the TOE have been clarified by a table *Limits of the TOE* were usage and construction of the TOE have been selected among the smart card phases.
- The Embedded Software cannot be extended during usage phases of the TOE but only during the construction phases of the TOE.
- The PP9810 covers the security of a generic SmartCard Embedded Software taken into account the management of the chip security features.
- Card Risk Management is based on the security of the Embedded Software.

This is the reason why there is no threats in addition to the PP9810 .

3.2 Organizational security policy

The TOE must use a chip which meets PP/9806 , the TOE will follow the chip User Guidance.

3.3 Assumptions

See PP/9810.

Here are security rules that are supposed to followed by all the administrators and users of the cards. Those rules may not be considered as organizational security policy as they cannot be checked by the evaluation process. Those rules deal mainly with phases 4,5,6,7 that are not the construction phases of the TOE but the usage phases of the TOE.

3.3.1 PIN MANAGEMENT

The end-user is the only actor to know the PIN in a deciphered way.

PIN code mailing must be separate from the card mailing.

A card must never be close to any document giving PIN contents.

These policies are relevant to phases 6 and 7.

3.3.2 UNIQUENESS OF CARDS

Cards must have a unique personalization, i.e. personalization must be operated with a process that prevents from fraudulent or unexpected cloning.

These policies are relevant to phases 6 .

3.3.3 VALIDITY OF CARDS

Card must be issued with a maximum validity of 3 years.

These policies are relevant to phases 6 and 7

3.3.4 TERMINALS

Terminals must be protected against fraudulent storage or tapping of the PIN

The public key stored in the terminal is protected against malicious over-write.

These policies are relevant to phases 7.

3.3.5 SECRET KEYS MANAGEMENT

The card issuer and card administrators servers must keep the all application secret keys with a high level of confidentiality.

These policies are relevant to phases 5,6 and 7.

3.3.6 TRANSACTION CONTROL

The transaction contents must be archived in case of repudiation or any other dispute.

The off-line transactions signatures must be audited .

These policies are relevant to phases 7.

4. TOE SECURITY OBJECTIVES

See PP/9810.

5. TOE SECURITY REQUIREMENTS

5.1 TOE security functional requirements

The TOE Security functional requirements define the functional requirements for the TOE using only functional requirements components drawn from CC part 2.

All operations such as iteration, assignment, selection and refinement have been performed. The minimum strength level for the TOE security functions is SOF-high.

5.1.1 SECURITY AUDIT AUTOMATIC RESPONSE (FAU_ARP)

5.1.1.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1 The TSF shall take **actions among the following list** upon detection of a potential security violation:

1. **Clear the RAM, stop execution until the next session;**
2. **Disable the TOE;**
3. **Flash program the EEPROM, clear the RAM, stop execution until the next session ;**

5.1.2 SECURITY AUDIT ANALYSIS (FAU_SAA)

5.1.2.1 FAU_SAA.1 Potential violation analysis

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events :

a) Accumulation or combination of the following auditable events known to indicate a potential security violation:

1. **Change of operation voltage;**
2. **Instantaneous clock frequency below the minimum authorised value or above the maximum specified value;**
3. **Unauthorised access to memories;**
4. **Unauthorised call to System ROM;**
5. **Bad EEPROM sequences;**
6. **Bad Opcode execution;**
7. **Card Life Cycle Status discrepancy;**
8. **EEPROM programming failure;**
9. **File structure integrity failure;**
10. **Authentication data integrity failure;**

b) Other rule: **none.**

5.1.3 CRYPTOGRAPHIC KEY MANAGEMENT (FCS_CKM)

5.1.3.1 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1/RDR The TSF shall perform **cryptographic key reading** in accordance with a specified cryptographic key access method**, Random Reading Method** that meets the following standard : **none**.

FCS_CKM.3.1/UPT The TSF shall perform **cryptographic key creation** in accordance with a specified cryptographic key access method, **Balanced Storage Method** that meets the following standard : **none**.

5.1.3.2 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, **Stable Erase Method** that meets the following standard : **none**.

5.1.4 CRYPTOGRAPHIC OPERATIONS (FCS_COP)

5.1.4.1 FCS_COP.1 Cryptographic operations

FCS_COP.1.1/CIPH The TSF shall perform **deciphering of input ciphered data** in accordance with a specified cryptographic algorithm, **triple DES in CBC mode (phases 4 to 6) and in ECB mode (phase 7)** and cryptographic key size of **16 bytes** that meet the following standards : **ANSI X3.92 and VIS 1.3.1 (Only in phase 7)**.

FCS_COP.1.1/MAC The TSF shall perform **cryptographic Administrator Authentication cryptogram computation and MAC computation for Secure Messaging** in accordance with a specified cryptographic algorithm, **DES in CBC mode combined with triple DES in CBC mode (CBC-MAC algorithm)** and cryptographic key size of **16 bytes** that meet the following standards: **ANSI X3.92 and VIS 1.3.1 (Only in phase 7)**.

5.1.5 ACCESS CONTROL POLICY (FDP_ACC)

5.1.5.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1/CMD The TSF shall enforce the **Command Access Control SFP** on the **subject SUB_CMDMAN** and **all the objects SUB_CMD**, and all operations among

subjects and objects covered by the SFP.

Command Access Control SFP :

- **Operations : activation of SUB_CMD by SUB_CMDMAN;**
- **Only SUB_CMDMAN can activate a SUB_CMD upon receipt of a command message;**
- **SUB_CMD shall be activated only if the command message corresponds to a supported internal process and is valid;**
- **The user shall be authenticated as an Administrator to allow activation by SUB_CMDMAN of administrator-reserved SUB_CMD;**

Definitions :

SUB_CMDMAN	**Process that receives and interpret the command messages sent by the remote IT product.**
SUB_CMD	**Process activated on SUB_CMDMAN request according to a specific command message.**

Refinement*: Once the card initialisation phase is completed, the TOE, does not allow the creation of SUB_CMD subjects.*

FDP_ACC.2.2/CMD The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACC.2.1/FILE The TSF shall enforce the **File Access Control SFP** on **all the subjects SUB_CMD that allow direct access to object OB_DFILE and E_FILE,** and **all the objects OB_DFILE and OB_EFILE**, and all operations among subjects and objects covered by the SFP.

File Access Control SFP :

- **Operations : creation of OB_EFILE or OB_DFILE stored in OB_DFILE by SUB_CMD, creation, update and read of data element(s) stored in OB_EFILE by SUB_CMD; these operations concern data exchange with the current user of the TOE, not the TOE internal exchanges;**
- **SUB_CMD shall create OB_EFILE or OB_DFILE in OB_DFILE only if the access conditions of OB_DFILE are fulfilled;**
- **SUB_CMD shall have access to data element(s) stored in OB_EFILE only if the access conditions of the file are fulfilled;**

Definitions :

OB_DFILE	**Dedicated File; entity in EEPROM containing other(s) objects OB_EFILE or OB_DFILE, that is part of the TOE file structure.**
OB_EFILE	**Elementary File; entity in EEPROM containing user or TSF data, that is part of the TOE file structure.**

FDP_ACC.2.2/FILE The TSF shall ensure that all operations between any subject in the TSC and any

object within the TSC are covered by an access control SFP.

FDP_ACC.2.1/SEC The TSF shall enforce the **Secret Access Control SFP** on **all the subjects SUB_CRYPTALGO and SUB_CMD** and **all the objects OB_KEY and OB_PIN**, and all operations among subjects and objects covered by the SFP.

Secret Access Control SFP :

- **Operations : read, update of OB_KEY and OB_PIN by a command SUB_CMD, use of a key stored in OB_KEY, resp. a PIN stored in OB_PIN, by a cryptographic algorithm SUB_CRYPTALGO, resp. a command SUB_CMD;**
- **Use of a key by an algorithm is allowed only if they have the same type;**
- **Use of a cryptographic key or a PIN is allowed only if it is not blocked;**
- **Cryptographic key and PIN shall not be read by any user;**
- **PIN shall only be updated by the Administrator;**
- **Cryptographic key shall not be updated;**

Definitions :

SUB_CRYPTALGO	**Process performing cryptographic computation.**
OB_KEY	**Entity in EEPROM containing a cryptographic key. May be stored in a OB_EFILE (TSF Data).**
OB_PIN	**Entity in EEPROM containing the PIN. Stored in a OB_EFILE (TSF Data).**

FDP_ACC.2.2/SEC The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACC.2.1/TLV The TSF shall enforce the **Application Proprietary TLV Object Access Control SFP** on **all the subjects SUB_CMD** and **all the objects OB_APTLV**, and all operations among subjects and objects covered by the SFP.

Application Proprietary TLV Object Access Control SFP :

- **Operations : update and read of data element stored in OB_APTLV by SUB_CMD; these operations concern data exchange with the current user of the TOE, not the TOE internal exchanges;**
- **SUB_CMD shall have access to data element stored in OB_APTLV only if the tag associated to the data element belongs to the relevant access list;**
- **Update of OB_APTLV shall be performed using Secure Messaging;**
- **Update of OB_APTLV shall be performed during phase 7 only;**

Definition :

OB_APTLV	**Entity in EEPROM containing an Application Proprietary TLV Object data object (user data).**

FDP_ACC.2.2/TLV The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

5.1.6 ACCESS CONTROL FUNCTIONS (FDP_ACF)

5.1.6.1 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1/CMD The TSF shall enforce the **Command Access Control SFP** to objects based on the **Card Life Cycle Status, Card Security Status group, Command Life Cycle, Command Header Format and Command Key security attributes**.

FDP_ACF.1.2/CMD The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed :

1. **SUB_CMDMAN shall activate SUB_CMD only if the Command Life Cycle security attribute is consistent with the Card Life Cycle Status;**
2. **SUB_CMDMAN shall activate SUB_CMD only if the Command Header Format, i.e. class, instruction, parameters P1 to P3, is valid;**
3. **SUB_CMDMAN shall activate SUB_CMD only if the Command Key security attribute matches the Card Security Status group;**

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

FDP_ACF.1.4/CMD The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none.**

FDP_ACF.1.1/FILE The TSF shall enforce the **File Access Control SFP** to objects based on the **Command File Type, File Access Conditions, File Type and Card Security Status group of security attributes**.

The Card Security Status group consists in the following attributes : {Pin Security Status, Key Security Status, Secure Messaging Status}.

FDP_ACF.1.2/FILE The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed :

1. **Any SUB_CMD shall have access to OB_DFILE or OB_EFILE only if the Command File Type security attribute matches the File Type security**

attribute;

2. **Any SUB_CMD shall have access to OB_DFILE or OB_EFILE only if the corresponding access condition of the File Access Conditions security attribute is fulfilled according to the Card Security Status group;**

FDP_ACF.1.3/FILE The TSF shall explicitly authorize access of subjects to objects based on the following additional rules :

1. The object is an OB_EFILE object, an update access to the first data element stored in OB_EFILE is requested, the TOE is in phase 7, the Command File Type security attribute matches the File Type security attribute and the SFI of OB_EFILE is equal to 1**..**

FDP_ACF.1.4/FILE The TSF shall explicitly deny access of subjects to objects based on the following additional rules : **none.**

FDP_ACF.1.1/SEC The TSF shall enforce the **Secret Access Control SFP** to objects based on the **Cryptographic Algorithm Type, Key Type and Ratification group of security attributes**.

The Ratification group consists in the following security attributes : {Maximum Presentation Number, Ratification Counter}.

FDP_ACF.1.2/SEC The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed :

1. **Any SUB_CRYPTALGO shall use a key only if the Key Type security attribute matches the Cryptographic Algorithm Type;**
2. **Any SUB_CRYPTALGO shall use a key only if the Ratification group does not indicate the key is blocked;**
3. **Any SUB_CMD shall use a PIN only if the Ratification group does not indicate the PIN is blocked;**

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

FDP_ACF.1.4/SEC The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. **No SUB_CMD shall have update access to OB_KEY;**
2. **No SUB_CMD shall have update access to OB_PIN during phases 4 to 6;**
3. **No SUB_CMD shall have read access to OB_KEY and OB_PIN;**

FDP_ACF.1.1/TLV The TSF shall enforce the **Application Proprietary TLV Object Access Control SFP** to objects based on the **Card Life Cycle Status, TLV Life cycle, TLV Read Access List and TLV Update Access List security attributes**.

FDP_ACF.1.2/TLV The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed :

1. **Any SUB_CMD shall have read access to OB_APTLV only if the tag associated to the object belongs to the TLV Read Access List security attribute;**
2. **Any SUB_CMD shall have update access to OB_APTLV only if the tag associated to the object belongs to the TLV Update Access List security attribute;**
3. **Any SUB_CMD shall have access to OB_APTLV only if the TLV Life cycle security attribute is consistent with the Card Life Cycle Status security attribute;**

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

FDP_ACF.1.4/TLV The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. **Secure Messaging is not used to update OB_APTLV;**
2. **The TOE is not in phase 7 and update access is requested;**

5.1.7 DATA AUTHENTICATION (FDP_DAU)

5.1.7.1 FDP_DAU.1 Basic data authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **the File Attributes and Application Proprietary TLV Objects.**

FDP_DAU.1.2 The TSF shall provide **all the subjects SUB_CMD** with the ability to verify evidence of the validity of the indicated information.

5.1.8 EXPORT TO OUTSIDE TSF CONTROL (FDP_ETC)

5.1.8.1 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the **File Access Control and Application Proprietary TLV Object Access Control SFPs** when exporting user data, controlled under the SFP, outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

5.1.9 IMPORT FROM OUTSIDE TSF CONTROL (FDP_ITC)

5.1.9.1 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **File Access Control and Application Proprietary TLV Object Access Control SFPs** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore the 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 : **none.**

5.1.10 RESIDUAL INFORMATION PROTECTION(FDP_RIP)

5.1.10.1 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource** to the following objects : **OB_CRYPTBUF, OB_CMDBUF**.

Definition :

OB_CRYPTBUF	**Entity in RAM containing cryptographic variables used for cryptographic computation.**
OB_CMDBUF	**Entity in RAM containing data used for command processing.**

5.1.11 STORED DATA INTEGRITY (FDP_SDI)

5.1.11.1 FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for **LRC integrity error** on all objects, based on the following attributes :

1. **File Header LRC**
2. **Application Proprietary TLV Object LRC**

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **deny the use of the corrupted data.**

5.1.12 AUTHENTICATION FAILURES (FIA_AFL)

5.1.12.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when a number that can be configure by an authorized administrator between 1 and 15 of unsuccessful authentication attempts occur related to the Administrator Authentication and End-User authentication during phase 7

FIA_AFL.1.2 When the defined number of unsuccessful attempts has been met or surpassed, the TSF shall perform the following actions, **depending on the authentication event :**

1. **Administrator Authentication: definitely deny the use of the cryptographic key for further authentications;**
2. **End-User authentication (phase 7) : deny the use of the PIN for further authentications until the PIN is unblocked by an authorized Administrator;**

5.1.13 USER ATTRIBUTE DEFINITION (FIA_ATD)

5.1.13.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users : **Card Security Status group = {Pin Security Status, Key Security Status, Secure Messaging Status}.**

5.1.14 USER AUTHENTICATION (FIA_UAU)

5.1.14.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **all the TSF mediated actions except the following list** on behalf of the user to be performed before the user is authenticated:

1. **User and TSF data loading;**
2. **User and TSF data updating;**

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.

5.1.14.2 FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1 The TSF shall **detect and prevent** use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall **prevent** use of authentication data that has been copied from any other user of the TSF.

Refinement : this requirement does not include PIN since it is impossible for the TSF to prevent the sharing of PIN outside the control of the TSF.

5.1.14.3 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to **the Administrator Authentication mechanism during phases 4 to 6**.

5.1.15 USER IDENTIFICATION (FIA_UID)

5.1.15.1 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **all TSF mediated actions** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.16 USER-SUBJECT BINDING (FIA_USB)

5.1.16.1 FIA_USB.1 User-subject binding

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

5.1.17 MANAGEMENT OF FUNCTION IN THE TSF (FMT_MOF)

5.1.17.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **modify the behaviour** of the **following** functions to the **Administrator role and to phases 4 to 6:**

1. **Administrator Authentication SF_AUTH;**
2. **Secure Secret Data Loading SF_SLD;**

5.1.18 MANAGEMENT OF SECURITY ATTRIBUTES (FMT_MSA)

5.1.18.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1/FILE The TSF shall enforce the **Command Access Control and File Access Control SFPs** to restrict the ability to **create** the security attribute **File Type to the Administrator role and to phases 4 to 6.**

FMT_MSA.1.1/SEC The TSF shall enforce the **Command Access Control and Secret Access Control SFPs** to restrict the ability to **perform the following operations on the following** security attributes **to the Administrator role and to the following phases.**

Security attribute	**Operation**	**Phase(s)**
Key Type	Create	4 to 6
Ratification group	Create	4 to 6
Ratification counter	reset to Maximum Presentation Number	7

5.1.18.2 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.18.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1/CMD The TSF shall enforce the **Command Access Control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/CMD The TSF **shall** allow no role to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1/FILE The TSF shall enforce the **File Access Control SFP** to provide **the following property for** default values for security attributes that are used to enforce the SFP.

Property : no default values are supported except for the following security attributes.

1. **The Card Security Status group is set to {'no','no','no'} at the beginning of each session;**

The Command File Type security attribute is set during ES development and cannot be changed.

The security attributes File Type, Key Type, Ratification group must be provided by the Administrator when the object is created.

The security attribute File Access Conditions is derived from File Type therefore the Administrator shall not provide this security attribute.

FMT_MSA.3.2/FILE The TSF shall allow **no role** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1/SEC The TSF shall enforce the **Secret Access Control SFP** to provide **the following property for** default values for security attributes that are used to enforce the SFP.

Property : no default values are supported.

The Cryptographic Algorithm Type security attribute is set during ES development and cannot be changed.

The security attributes Key Type and Ratification group must be provided by the Administrator when the object is created.

FMT_MSA.3.2/SEC The TSF shall allow the **no role** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.1/TLV The TSF shall enforce the **Application Proprietary TLV Object Access Control SFP** to provide **the following property for** default values for security attributes

that are used to enforce the SFP.

Property : no default values are supported.

The TLV Life cycle, TLV Read Access List and TLV Update Access List security attributes are set during ES development and cannot be changed.

FMT_MSA.3.2/TLV The TSF shall allow **no role** to specify alternative initial values to override the default values when an object or information is created.

5.1.19 MANAGEMENT OF TSF DATA (FMT_MTD)

5.1.19.1 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **perform the following actions on** the **following** TSF data to the **Administrator role and to the indicated phases:**

1. **Create cryptographic key (phases 4 to 6);**
2. **Create PIN (phases 4 to 6);**
3. **Update PIN (phase 7);**
4. **Unblock PIN by setting the PIN Ratification Counter to the PIN Maximum Presentation Number (phase 7);**

5.1.20 SECURITY MANAGEMENT ROLES (FMT_SMR)

5.1.20.1 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the **following** roles :

1. **Administrator: this role has capabilities defined by proving the knowledge of secret cryptographic keys, depending on the logical phase of the TOE; during phases 4 to 6, the Administrator role has the capability to create File objects, load and update user and TSF data after performing a successful Administrator Authentication; during phase 7, the Administrator role has the capability to update user and TSF data using the Secure Messaging mechanism;**
2. **End-User: this role has limited capabilities because proving the knowledge of secret cryptographic keys cannot be done; during phases 4 to 6, the End-User role cannot create File objects, load nor update user and TSF data; during phase 7, the End-User role has limited capability to update user data, under control of the access rules defined during phases 4 to 6 by the Administrator;**

FMT_SMR.1.2 **The TSF shall be able to associate users with roles.**

5.1.21 CLASS FMT : ACTIONS TO BE TAKEN FOR MANAGEMENT

Function	Actions
FCS_CKM.3	Managing changes to cryptographic key attributes (user, type, validity, use ...)
FCS_CKM.4	Managing changes to cryptographic key attributes (user, type, validity, use ...)
FDP_ACF.1	Managing the attributes used to make explicit access or denial based decisions
FDP_DAU.1	Assignment or modification of the objects for which data authentication may apply could be configurable in the system
FDP_ITC.1	The modification of the additional control rules used for import
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts
FIA_UAU.1	Management of the authentication data by an administrator
FIA_USB.1	An authorized administrator can define default subject security attributes
FMT_MOF.1	Managing the group of roles that can interact with the functions in the TSF
FMT_MSA.1	Managing the group of roles that can interact with the security attributes
FMT_MSA.3	Managing the group of roles that can specify initial values
FMT_MTD.1	Managing the group of roles that can interact with the TSF data

5.1.22 UNOBSERVABILITY (FPR_UNO)

5.1.22.1 FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure **any user is** unable to observe the **following** operations on **the following objects** by **the following subjects**.

In this security target, unobservability means impossibility to obtain the address and / or the value of an information during an operation on this information.

Subject	Operation	Object
SUB_CMD	**create/update PIN**	**OB_PIN**
SUB_CMD	**create key**	**OB_KEY**
SUB_CMD	**comparison of PIN value with reference**	**OB_PIN**
SUB_CRYPTALGO	**use**	**OB_KEY**

5.1.23 Fail secure (FPT_FLS)5.1.23.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures

occur :

1. **Unexpected abortion of the execution of the TSF due to external events;**
2. **File structure integrity failure;**
3. **Authentication data integrity failure;**
4. **Card Life Cycle Status discrepancy;**
5. **EEPROM flash program;**
6. **EEPROM programming failure;**

5.1.24 TSF PHYSICAL PROTECTION (FPT_PHP)

5.1.24.1 FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist the **following physical tampering scenarios** to the **following TSF elements** by responding automatically such that the TSP is not violated.

Element	Physical tampering scenario	Automatic response
Card Life Cycle Status	**Erasure**	**Flash program the EEPROM, clear the RAM and run an infinite loop**
Clock	**Reduction of clock frequency to stop the TOE during a specific operation**	**Account the event to trigger shield action**
Clock	**Increase clock frequency to corrupt TOE operation behavior**	**Account the event to trigger shield action**
Voltage supply	**Set supply voltage out of range**	**Account the event to trigger shield action**

5.1.25 DOMAIN SEPARATION (FPT_SEP)

5.1.25.1 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.

5.1.26 INTER-TSF BASIC DATA CONSISTENCY (FPT_TDC)

5.1.26.1 FPT_TDC.1 Inter-TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **Key and PIN data** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use the following interpretation rules when interpreting the TSF data from another trusted IT product:

1. **Key loading (phases 4 to 6) : key data consists in a header containing the key attributes and a body containing the key value; this data block is ciphered and signed using Secure Messaging mechanism;**
2. **PIN loading (phases 4 to 6) : PIN data consists in a header containing the PIN attributes and a body containing the PIN value; this data block is ciphered and signed using Secure Messaging mechanism;**

5.1.27 TSF SELF TEST (FPT_TST)

5.1.27.1 TSF Testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests **at the following conditions** to demonstrate the correct operation of the TSF:

1. **At startup;**
2. **After receiving a command message;**
3. **Before and during programming or erasing the EEPROM;**

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of the stored TSF executable code.

5.2 TOE security assurance requirements

See PP/9810.

6. TOE SUMMARY SPECIFICATIONS

This section defines the instantiation of the security requirements for the TOE.

6.1 TOE security functions

6.1.1 SF_ACC : DATA ACCESS CONTROL

This SF manages the access to the data elements by the command subjects SUB_CMD. The data elements can be stored either in records inside a file or in TLV encoded objects.

Dedicated File access

This SF ensures the following :

– Check the file type is supported;

– Determine during file creation the access conditions according to the file type;

– Allow the required access to the file if the relevant access conditions are fulfilled and the file header is valid;

The following access condition is attached to each DF : AC_CREATE. This access condition applies to all the data elements stored in the file.

Access Condition	Access Description
AC_CREATE	Create an EF or DF under the DF

The possible values of the access condition are listed below :

Access Condition value	Description
FREE	Access is always allowed
NEVER	Access is never allowed
CHV	Successful PIN presentation required
SMI	The command requiring access shall use the Secure Messaging for Integrity format and the associated MAC shall be correct.
SMC	The command requiring access shall use the Secure Messaging for Integrity and Confidentiality format and the associated MAC shall be correct.

Elementary File access

This SF ensures the following :

– Check the file type is supported;

– Determine during file creation the access conditions according to the file type;

– Allow the required access to the file if the relevant access conditions are fulfilled and the file header is valid;

The following access conditions are attached to each file : AC_APPEND, AC_UPDATE and AC_READ. These access conditions apply to all the data elements stored in the file.

Access Condition	Access Description
AC_APPEND	Add a data element in the file
AC_UPDATE	Update a data element in the file
AC_READ	Read a data element in the file

Special case : the update access to the first data element stored in the file is allowed whatever the AC_UPDATE access condition if the TOE is in phase 7, the file type is supported and the SFI of the file is equal to 1.

The possible values of an access condition are listed below :

Access Condition value	Description
FREE	Access is always allowed
NEVER	Access is never allowed
CHV	Successful PIN presentation required
SMI	The command requiring access shall use the Secure Messaging for Integrity format and the associated MAC shall be correct.
SMC	The command requiring access shall use the Secure Messaging for Integrity and Confidentiality format and the associated MAC shall be correct.

TLV access

This SF ensures the following :

– Allow the required access to the TLV object if the tag is in the relevant access list, the access to the object is permitted for the current TOE phase and the TLV object is valid;

– Deny any update access if the TOE is not in phase 7;

The following access lists are maintained by the SF : ACL_GET, ACL_PUTSM.

Access List	**Access Description**
ACL_GET	Read a TLV object
ACL_PUTSM	Update a TLV object; the command requiring access shall use the Secure Messaging for Integrity format and the associated MAC shall be correct

6.1.2 SF_AUTH : ADMINISTRATOR AUTHENTICATION

This function ensures the management of the Administrator Authentication. This function is realized by a permutational mechanism. The strength of the function is SOF-high.

Phases 4 to 6 :

The user is authenticated as the Administrator through the Administrator Authentication mechanism, based on cryptographic challenge-response protocol. The authentication cryptogram provided by the user is computed using the CBC-MAC algorithm and a double length key on the following input data :

– User generated random number;

– TOE generated random number;

– Unique TOE identifier;

The size of the input data shall be greater than the size of the authentication cryptogram.

The number of attempts is limited by the ratification counter associated to the key used for cryptographic computation. This counter is decremented each time the authentication fails; the key cannot be used for authentication any longer if the counter reaches zero. If the authentication is successful, the ratification counter is set to the maximum presentation number of the key.

The double length key used for computation depends on the TOE logical phase :

– **Phases 4 and 5** : diversified key stored in the EEPROM by the chip manufacturer;

– **Phase 6** : authentication diversified key stored in a key file by the smartcard product manufacturer;

Phase 7 :

The user is authenticated as the Administrator through the use of the Secure Messaging mechanism, which is based on secret cryptographic key sharing. The authentication cryptogram provided by the user is computed using the CBC-MAC algorithm on the following input data :

– Command header;

– Last ATC;

– Last AC;

– Plain text or ciphered data;

– Padding;

If the authentication cryptogram is wrong, further Administrator authentications are rejected until the end of the transaction.

The number of attempts is limited by the ratification counter associated to the key used for cryptographic computation. This counter is decremented each time the authentication fails; the key cannot be used for authentication any longer if the counter reaches zero. If the authentication is successful, the ratification counter is set to the maximum presentation number of the key.

6.1.3 SF_BKP : BACKUP MANAGEMENT

This function ensures the management of secure data element update in EEPROM :

– Backup operation : copy the contents of EEPROM cells containing sensitive data in the backup dedicated EEPROM area before update;

– Invalidate the copied data in the dedicated area after successful update;

– Rollback operation : restore the copied data in case of update failure, i.e. uncompleted EEPROM programming sequence, or on request of the ES;

The SF ensures the EEPROM containing sensitive data is in a coherent state whatever the time when EEPROM programming sequence stops, either during copying, invalidating, restoring data to or from the backup dedicated EEPROM area or updating sensitive data in EEPROM.

If an EEPROM programming failure occurs during backup or rollback, the event is notified to SF_DRV.

6.1.4 SF_CMDMAN : COMMAND MANAGEMENT

This function controls the execution of the card internal process corresponding to command messages sent by the user to the card :

– Startup management : the TOE configuration is checked, the command and cryptographic buffers are created;

– Identification : the instruction code of the command message is supported;

– Format analysis : the class shall be consistent with the instruction code, P1/P2/P3 parameters values shall be supported by the identified command;

– Life cycle analysis : the identified command shall be enabled in the current life cycle phase of the TOE;

– Access conditions : if the command is administrator-reserved, check the user has been authenticated as administrator. The authentication can be performed before processing the command message, using other messages for positive authentication, and/or when receiving the command message, using Secure Messaging mechanism;

– Execution : activation of the executable code corresponding to the card internal process for the command message;

– Sensitive buffers management : the command buffer is cleared after each command, the cryptographic buffer is cleared after completion of cryptographic computation;

6.1.5 SF_CMP : SECURE COMPARISON

This function ensures the comparison between two data elements is unobservable.

6.1.6 SF_CRY : CRYPTOGRAPHIC COMPUTATION

This function ensures the following cryptographic computations :

– Session key generation;

- Data deciphering : triple DES in CBC mode (phase 4 to 6) or in ECB mode (phase 7) using a double length session key; Conformance to VIS 1.3 only in phase 7.
- Secure Messaging MAC computation : CBC-MAC using a double length session key;
- Administrator Authentication cryptogram computation : CBC-MAC using a double length session key;
- Application Cryptogram computation : CBC-MAC using a double length key;

6.1.7 SF_DRV : CHIP DRIVER

This function ensures the management of the chip security features :

- Start state analysis;
- Record audit events;
- Perform shield actions according to violation severity;
- Control random clock generation;

The following auditable events are accounted during a session :

1. Change of operation voltage;
2. Instantaneous clock frequency below the minimum authorized value or above the maximum specified value;
3. EEPROM programming failure during backup/rollback;
4. File structure integrity failure;
5. Authentication data integrity failure;

This function performs TOE state analysis at startup. It is able to determine the following auditable events have occurred previously at the beginning of a session :

1. Unauthorized access to memories (warm reset only);
2. Unauthorized call to System ROM (warm reset only);
3. Bad EEPROM sequences (warm reset only);
4. Bad Opcode execution (warm reset only);
5. Card Life Cycle Status discrepancy;

This SF makes decision on the basis of accumulation or combination of auditable events and perform the following relevant shield actions when a potential violation is detected :

Violation	**Shield action**
• EEPROM programming failure during backup/rollback • File structure integrity failure • Authentication data integrity failure	1.Disable the TOE 2.Clear the RAM 3.Stop execution until the next session
• Change of operation voltage • Instantaneous clock frequency below the minimum authorized value [IC] • Instantaneous clock frequency above the maximum specified value	1.Clear the RAM 2.Stop execution until the next session
• Unauthorized access to memories [IC] • Unauthorized call to System ROM [IC] • Bad Opcode execution [IC] • Bad EEPROM sequences [IC] • Card Life Cycle Status discrepancy	1.Flash program the EEPROM 2.Clear the RAM 3.Stop execution until the next session

How to read this table:

For each row, one of the detected violation (left cell) makes the TOE to take all the shield actions numbered in the right cell. (For instance: ‘Change of operation voltage’ is replied by ‘1.Clear the RAM’ and ‘2.Stop execution until the next session’.)

The mark ‘[IC]’, indicates that the violation is detected by the chip itself, then the shield action is always taken by the operating system. When not specified, the violation is detected by the operating system.

The ‘Flash program the EEPROM’ and the ‘Clear the RAM’ actions are implemented by the Chip itself.

This SF controls the clock generation to create variations of the CPU clock. These variations and their occurrences are not predictable. This feature is enabled during sensitive data processing and disabled during communication and EEPROM programming.

6.1.8 SF_INT : DATA INTEGRITY

This function provides the ability to check the integrity of the following data elements stored in EEPROM :

– File header, containing the file attributes (identifier, size, type, access conditions, status, chaining information, header LRC);

– PIN value and header, containing the PIN attributes (maximum presentation number, ratification, size, PIN LRC);

– Key value and header, containing the key attributes (maximum presentation number, ratification, size, key type, key LRC);

– Application Proprietary TLV Object objects;

6.1.9 SF_KEY : CRYPTOGRAPHIC KEY MANAGEMENT

This function controls all the operations relative to the cryptographic key management :

- Key search : depends on the card life status; the key can be stored either in a specific location in the EEPROM or in a Key file;
- Key verification : the key can be accessed only if its format and integrity are correct;
- Key read : the key can be read only if it is not blocked and its type matches the requested type; the key is transferred from EEPROM to RAM using the Random Reading Method. The bytes composing the key value are read in random order and stored in the actual order. Moreover, the additional information added by the Balanced Storage Method is removed;
- Key creation : the key is transferred from RAM to EEPROM using the Balanced Storage Method. Additional information is added to the key in order to equalize the Hamming weight of each bytes of the key.;
- Key destruction : the EEPROM cells storing the key value are programmed with the stable state of the EEPROM cells;
- Key ratification management : decrementation of the key ratification counter before use and reset to the maximum presentation number in case of successful use;

6.1.10 SF_LOCK : CARD LIFE STATUS MANAGEMENT

This function ensures the management of the TOE life cycle. The chronological phases 4 to 7, defined in section 0, are managed by this SF. The TOE is able to determine the current phase and to change from one to the next one.

1. Check the integrity of the Card Life Cycle Status;
2. Determine the current phase in which the TOE is;
3. Change to next phase : this change is irreversible;

If the Card Life Cycle Status is corrupted, then the event is notified to SF_DRV.

6.1.11 SF_PIN : PIN MANAGEMENT

This function controls all the operations relative to the PIN management, including the End-User authentication:

- PIN search : the PIN is stored in a PIN file, which may exist either under the DF of the current active application or under the MF;
- PIN verification : the PIN can be accessed only if its format and integrity are correct. If the PIN is blocked, then it cannot be used except for unblocking and changing;
- End-User Authentication : PIN comparison with reference supplied by the End-User for authentication purpose; the length of the PIN is between 4 and 16 digits; the number of attempts is limited by the ratification counter associated to the PIN; this counter is decremented each time the authentication fails; the PIN cannot be used for authentication any longer if the counter reaches zero;
- PIN modification : the PIN can be unblocked (reset the ratification counter to the initial value) and changed (loading of a new value);

This function is realized by a permutational mechanism (EndUser authentication= PIN). The strength of this function is SOF-high.

6.1.12 SF_RAT : RATIFICATION MANAGEMENT

This function ensures the management of the ratification counters associated with PIN and cryptographic keys :

– Ratification read;

– Ratification decrease;

– Ratification reset to the maximum authorized value;

6.1.13 SF_SEC : SECURITY MANAGEMENT

This function maintains the security attributes of the user. Because the TOE cannot identify the user by analyzing the command message(s), only one group of user security attributes is maintained during a session.

The result of interpreting the command message(s) is the activation of subject(s) SUB_CMD, acting on behalf of the user. The user security attributes are associated to the subject, and are identical to the Card Security Status group of security attributes.

This SF updates the Card Security Status group according to the processed commands using the following rules :

– Reset the group of security attributes Card Security Status {Pin Security Status, Key Security Status, Secure Messaging Status} to {'no','no','no'} at the beginning of a new session;

– Set the security attribute PIN Security status to 'yes' if a PIN is successfully presented;

– Reset the security attribute PIN Security status to 'no' if the current selected DF changes;

– Set the security attribute Key Security status to 'yes' if the Administrator Authentication is successful during phases 4 to 6;

– Set the Secure Messaging Status to 'yes' if the current command message uses a valid Secure Messaging format;

– Reset the Secure Messaging Status to 'no' after processing the current command message;

6.1.14 SF_SLD : SECURE SECRET DATA LOADING

This function ensures:

the secure loading of the PIN and keys while guaranteeing their integrity and confidentiality during phases 4 to 6.

- the secure update of the PIN while guaranteeing its integrity and confidentiality during phase 7.

This function is realized by a permutational mechanism, Secure Messaging applied to a dedicated command message. The strength of the function is SOF-high.

Phases 4 to 6

The secret data (PIN or key value and its associated attributes) is ciphered using the triple DES algorithm in CBC mode and a confidentiality session key.

This ciphered data is concatenated with the command message header and a random number generated by the TOE. After padding addition, the MAC is computed using the CBC-MAC algorithm and an integrity session key.

Both session keys are computed from a random number specific to the command message using the triple DES algorithm and a key depending on the TOE phase :

– **Phases 4 and 5** : integrity, resp. confidentiality, command specific key derived from the diversified key stored in the EEPROM by the chip manufacturer;

– **Phase 6** : integrity, resp. confidentiality, diversified key stored in a key file by the smartcard product manufacturer;

– **Phase 7 :** The secret data (PIN value) is ciphered using the triple DES algorithm in ECB mode and a confidentiality session key.

The Secure Messaging mechanism described in section 6.1.2 is used to build the complete command message. This allows to ensure the integrity of the message, in addition to the authentication of the Administrator

6.1.15 SF_TST : SELF TEST

This function ensures the following :

– Test the volatile memory is operating correctly on the beginning of a session;

– Compute a digital signature of the ROM code;

– Check the TOE configuration;

6.1.16 PERMUTATIONAL OR PROBABILISTIC SECURITY MECHANISMS

The following table demonstrates which security mechanisms are used in the implementation of each function.

	SF_ACC	SF_AUTH	SF_BKP	SF_CMDMAN	SF_CMP	SF_CRY	SF_DRV	SF_INT	SF_KEY	SF_LOCK	SF_PIN	SF_RAT	SF_SEC	SF_SLD	SF_TST
Administrator Authentication		x													
End-User Authentication											x				
Secure Messaging		X												x	

Table 6-1 : Mapping of the security mechanisms and the IT security functions

6.2 Assurance measures

Here is the list of required assurance.

These requirements are chosen to be consistent with an EAL4 assurance level

ASE
ADV_FSP.2
ADV_RCR.1 (1/4)
ADV_SPM.1
ADV_HLD.2
ADV_RCR.1 (2/4)
ADV_LLD.1
ADV_RCR.1 (3/4)
ADV_IMP.1

ADV_RCR.1 (4/4)
ATE
ATE_COV.2
ATE_DPT.1
ATE_FUN.1 **ATE**_IND.2
ACM_AUT.1 **ACM**_CAP.4 **ACM**_SCP.2
ACM_CAP.4 **ADO**_IGS.1
ACM_CAP.4 **ADO**_DEL.2
ALC_LCD.1
ALC_DVS.1
ALC_TAT.1
AGD_USR.1
AGD_ADM.1
AVA_MSU.2
AVA_SOF.1
AVA_VLA.2

7. PP CLAIMS

7.1 PP reference

This Security Target is inspired from the Protection Profile PP/9810 Version 1.2 dated November 19th '98 registered at the French Certification Body SCSSI. Nevertheless due to assurance level (EAL4) it is not compliant with the PP9810.

7.2 PP tailoring

This section identifies the IT security requirements statements that satisfy the permitted operations of the Protection Profile PP/9810.

The result of the performed operations is highlighted using bolding convention in the section 0.

Component	Iteration	Assignment	Selection	Refinement
FAU_ARP.1		x		
FAU_SAA.1		x		
FCS_CKM.3	X	x		

FCS_CKM.4		x		
FCS_COP.1	X	x		
FDP_ACC.2	X	x		
FDP_ACF.1	X	x		
FDP_DAU.1		x		
FDP_ETC.1		x		
FDP_ITC.1		x		
FDP_RIP.1		x	x	
FDP_SDI.2		x		
FIA_AFL.1		x		
FIA_ATD.1		x		
FIA_UAU.1		x		
FIA_UAU.3			x	x
FIA_UAU.4		x		
FIA_UID.1		x		
FIA_USB.1				
FMT_MOF.1		x	x	
FMT_MSA.1	X	x	x	
FMT_MSA.2				
FMT_MSA.3	X	x	x	
FMT_MTD.1		x	x	
FMT_SMR.1		x		
FPR_UNO.1		x		
FPT_FLS.1		x		
FPT_PHP.3		x		
FPT_SEP.1				
FPT_TDC.1		x		
FPT_TST.1		x	x	

Table 7-1 : Mapping of the performed operations and the IT security functional requirements

7.3 PP additions

There is no additional threats to the PP/9810 in this ST.

This ST defines the Organisational Security Policy :" Use a chip which meets PP/9806. As organisational Security policies are application dependent this is the only policy defined in this ST."

The ST adds the following TOE environment assumptions (described in §3.3) to the PP/9810 assumptions.

- Pin management (phase 6,7)
- Uniqueness of cards (phase 6)
- Validity of cards (phase 7)
- Terminals protection (phase 7)
- Secret Key management (phase 5,6,7)
- Transaction control (phase 7)

There is no additional security objectives and no additional requirements statements to the PP/9810 in this ST.

8. RATIONALE

The rationale is GEMPLUS property.

9. GLOSSARY

Access List

List of Application Proprietary TLV Objects for which a specific access is allowed.

Administrator

User that has the knowledge of the secret cryptographic keys stored in the TOE.

Application Cryptogram

Cryptogram generated by the TOE to authenticate a financial transaction.

Application Proprietary TLV Object

TLV object containing application-level data elements, stored in proprietary internal files. The data is LRC protected.

Application Transaction Counter

Unique identifier of a transaction for the TOE. Each transaction processed by the TOE has a different ATC.

Acquirer:

Organization between the Service Providers and the Bank of the Service Provider.

Blocking

A blocked secret (key or PIN) has its Ratification Counter security attribute set to zero : it cannot be used.

Card Issuer:

Bank that issues cards.

Card Life Cycle Status security attribute

Defines the current logical phase of the TOE.

Card Security Status group of security attributes

Defines the current security state associated to the user. It includes the following security attributes : {Pin Security Status, Key Security Status, Secure Messaging Status}.

Command File Type security attribute

Defines the file type(s) the command is allowed to access.

Command Life Cycle security attribute

Defines the availability of the command during each TOE logical phase from 4 to 7.

Command Header Format security attribute

Defines the allowed values of the class and parameters P1 to P3 for the command instruction code.

Command Key security attribute

Defines if a specific right shall be granted before executing the command.

Command

Executable code performing operations, possibly upon data stored in non-volatile memory, depending on the message received from the user accessing the TOE

Cryptographic Algorithm Type security attribute

Type of cryptographic algorithm (Administrator Authentication, Secure Messaging for integrity, Secure Messaging for confidentiality, application cryptogram generation).

Disabling

When the TOE is disabled, all the command messages except the one used for traceability information retrieval are rejected.

Embedded Software

The software embedded in the Smartcard Integrated Circuit. The ES may be in any part of the non-volatile memories of the Smartcard IC.

End-User

User that does not have the knowledge of the secret cryptographic keys stored in the TOE.

File Access

File access is defined as external access to the TOE data stored into a file.

Read access is the action of reading information stored and sending it outside the TSC.

Update, resp. write access is the action of updating, resp. adding, information stored using data coming from outside the TSC.

File Access Conditions security attribute

Security attributes defining the conditions that must be fulfilled in order to allow access to a file. Several types of access exists, depending on the kind of file, EF or DF.

File Header

Group of file attributes (file name, file type, size, identifier, file status, access conditions). These attributes are LRC protected.

File Object

Refers to two types of objects: OB_DFILE and OB_EFILE

File Type

File attribute defining the type of data stored in the file as well as the internal structure of the file.

Flash program

Fast programming of all the EEPROM cells with value FFh. Afterwards, the EEPROM is locked and cannot be modified.

Key Security Status security attribute

Is equal to 'yes' if the user has been successfully authenticated using the Administrator Authentication mechanism, else to 'no'.

Key Type security attribute

Type of cryptographic key (Administrator Authentication, Secure Messaging for integrity, Secure Messaging for confidentiality, application cryptogram generation).

Maximum Presentation Number security attribute

Initial value for the ratification counter associated to a secret (key or PIN). Used to reset the counter after a successful usage of the secret.

Merchant:

Service Provider:

Opcode

CPU instruction.

PIN Security Status security attribute

Is equal to 'yes' if the PIN has been successfully presented else to 'no'.

Payment Organization

Banks organization to ensure payment interoperability

Secure Messaging Status security attribute

Is equal to 'yes' if the current command message uses valid Secure Messaging format (MAC and possibly ciphered data), else to 'no'.

Ratification Counter security attribute

Counter associated to a secret (key or PIN), decremented in case of secret usage failure. Used to limit the number of attempts.

Ratification group security attribute

Group of security attributes associated to a secret (key or PIN). It includes the following security attributes : {Maximum Presentation Number, Ratification Counter}.

Reset

Warm reset : when the chip reset is due to a software or hardware interrupt occurring during a session.

Cold reset : when chip is reset occurs following standard power up conditions.

Session

Period between two consecutive cold or warm resets of the TOE.

Silicon Manufacturer.

Chip supplier called sometimes founder.

Short File Identifier

The 5 least significant bits of a file identifier.

Service Provider:

Organization that provides services to the end user, may be called merchant.

TLV Life cycle security attribute

Defines the TOE logical phases during the Application Proprietary TLV Object can be accessed.

TLV Read Access List security attribute

Defines the list of Application Proprietary TLV Objects that can be read by the user.

TLV Update Access List security attribute

Defines the list of Application Proprietary TLV Objects that can be updated by the user.

Transaction

Sequence of commands for performing a financial transaction, as specified in VIS 1.3.1 specification.

10. ABBREVIATIONS

AC

Application Cryptogram

ATC

Application Transaction Counter

CBC

Cipher-Block Chaining

CC

Common Criteria

DES

Data Encryption Standard

EAL

Evaluation Assurance Level

ECB

Electronic CodeBook

EEPROM

Electrically Erasable and Programmable Read Only Memory

EF

Elementary File

ES

Embedded Software

DF

Dedicated File

IT

Information Technology

LRC

Longitudinal Redundancy Checksum

MAC

Message Authentication Code

MF

Master file

PIN

Personal Identification Number

PP

Protection Profile

RAM

Random Access Memory

ROM

Read Only Memory

SF

Security Function

SFI

Short File Identifier

SFP

Security Function Policy

SOF

Strength Of Function

ST

Security Target

TLV

Tag Length Value

TOE

Target of Evaluation

TSC

TSF Scope of Control

TSF

TOE Security Functions

TSP

TOE Security Policy

11. REFERENCES

ES description	**Reference**	**Revision**
Gemplus Smart Debit/Credit	MST099	*
Chip description	**Reference**	**Revision**
ST19	ST19SF08AC RMY	*

* revisions are available in the Gemplus document: Documentation-List.01.

End Of Document.