 GEMPLUS	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 1/99

**Security Target
Gem CB-B0'/EMV**




	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 2/99

TABLE OF CONTENTS


1	<i>ST Introduction</i>	6
1.1	ST identification	6
1.2	ST overview	6
1.3	CC conformance claim	7
2	<i>TOE description</i>	7
2.1	Product type	7
2.1.1	EMV specifications	8
2.1.2	B0' specification	13
2.2	Smart card product life cycle	15
2.2.1	The TOE actors.....	16
2.2.2	TOE actors and roles	17
2.2.3	The limits of the TOE.....	18
2.3	TOE environment	18
2.3.1	TOE development environment	19
2.3.2	TOE Production Environment	19
2.3.3	TOE User Environment.....	19
2.4	TOE logical phases	20
2.5	TOE intended usage	21
3	<i>TOE Security environment</i>	22
3.1	Assets	22
3.2	Assumptions	22
3.2.1	Assumptions on phase 1	22
3.2.2	Assumptions on the TOE delivery process (phase 4 to 7)	23
3.2.3	Assumptions on phases 4 to 6.....	23
3.2.4	Assumptions on phase 7	23
3.3	Threats	24
3.3.1	Unauthorized full or partial cloning of the TOE.....	24
3.3.2	Threats on phase 1.....	24
3.3.3	Threats on delivery for/from phase 1 to phase 4 to 6.....	25
3.3.4	Threats on phases 4 to 7.....	26
3.4	Organizational security policy	28
4	<i>TOE SECURITY OBJECTIVES</i>	29
4.1	TOE Security Objectives	29
4.2	Environment Security objectives	30
4.2.1	Objectives on phase 1	30
4.2.2	Objectives on the Toe delivery process (phases 4 to 7)	30

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 3/99

4.2.3	Objectives on delivery from phase 1 to phase 4, 5 and 6.....	31
4.2.4	Objectives on phases 4 to 6.....	31
4.2.5	Objectives on phase 7	31
4.2.6	Additional objective for the IC.....	32
5	<i>TOE IT security functional requirements</i>	33
5.1	TOE security functional requirements for EMV application	33
5.1.1	Definition of EMV subject, objects and attributes.....	33
5.1.2	Security audit analysis (FAU_SAA).....	35
5.1.3	Non-repudiation of origin (FCO_NRO).....	36
5.1.4	Cryptographic key management (FCS_CKM).....	36
5.1.5	Cryptographic operations (FCS_COP).....	37
5.1.6	Access control policy (FDP_ACC)	37
5.1.7	Access control functions (FDP_ACF).....	40
5.1.8	Data authentication (FDP_DAU).....	43
5.1.9	Export to outside TSF control (FDP_ETC).....	43
5.1.10	Import from outside TSF control (FDP_ITC)	44
5.1.11	Residual information protection(FDP_RIP).....	44
5.1.12	Stored data integrity (FDP_SDI).....	44
5.1.13	Authentication failures (FIA_AFL).....	45
5.1.14	User attribute definition (FIA_ATD)	45
5.1.15	User authentication (FIA_UAU)	45
5.1.16	User identification (FIA_UID).....	46
5.1.17	User-subject binding (FIA_USB)	46
5.1.18	Management of function in the TSF (FMT_MOF).....	46
5.1.19	Management of security attributes (FMT_MSA).....	47
5.1.20	Management of TSF data (FMT_MTD).....	49
5.1.21	Security management roles (FMT_SMR).....	49
5.1.22	Class FMT : Actions to be taken for management.....	49
5.1.23	Unobservability (FPR_UNO).....	50
5.1.24	Fail secure (FPT_FLS)	50
5.1.25	TSF physical protection (FPT_PHP).....	51
5.1.26	Domain separation (FPT_SEP).....	51
5.1.27	Inter-TSF basic data consistency (FPT_TDC)	51
5.1.28	TSF self test (FPT_TST)	52
5.1.29	Inter-TSF trusted channel (FTP_ITC).....	52
5.2	TOE security functional requirements for B0' application	53
5.2.1	Definition of B0' subject, objects and attributes.....	53
5.2.2	Security audit analysis (FAU_SAA).....	56
5.2.3	Cryptographic key management (FCS_CKM).....	56
5.2.4	Cryptographic operations (FCS_COP).....	56
5.2.5	Access control policy (FDP_ACC)	57
5.2.6	Access control functions (FDP_ACF).....	59
5.2.7	Data authentication (FDP_DAU).....	62
5.2.8	Export to outside TSF control (FDP_ETC).....	62
5.2.9	Import from outside TSF control (FDP_ITC)	63
5.2.10	Residual information protection(FDP_RIP).....	63
5.2.11	Stored data integrity (FDP_SDI).....	63
5.2.12	Authentication failures (FIA_AFL).....	63
5.2.13	User attribute definition (FIA_ATD)	64

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 4/99

5.2.14	User authentication (FIA_UAU)	64
5.2.15	User identification (FIA_UID).....	65
5.2.16	User-subject binding (FIA_USB)	65
5.2.17	Management of function in the TSF (FMT_MOF).....	65
5.2.18	Management of security attributes (FMT_MSA).....	65
5.2.19	Management of TSF data (FMT_MTD).....	67
5.2.20	Security management roles (FMT_SMR).....	68
5.2.21	Class FMT : Actions to be taken for management.....	68
5.2.22	Unobservability (FPR_UNO).....	69
5.2.23	Fail secure (FPT_FLS)	69
5.2.24	TSF physical protection (FPT_PHP).....	69
5.2.25	Domain separation (FPT_SEP).....	70
5.2.26	Inter-TSF basic data consistency (FPT_TDC)	70
5.2.27	TSF self test (FPT_TST)	70
6	<i>TOE security assurance requirements</i>	71
6.1.1	Configuration management (ACM).....	71
6.1.2	Delivery and operation (ADO).....	71
6.1.3	Development (ADV)	71
6.1.4	Guidance document (AGD).....	71
6.1.5	Life cycle support (ALC).....	72
6.1.6	Tests (ATE).....	72
6.1.7	Vulnerability assessment (AVA).....	72
7	<i>TOE summary specifications</i>	73
7.1	Statement of TOE security function	73
7.1.1	Security function supplied by the IC	73
7.1.2	Security function for the platform.....	74
7.1.3	Statement of TOE security for EMV application	74
7.1.4	Statement of TOE security for B0' application	79
7.2	Statement of assurance measures	83
8	<i>PP claims</i>	84
8.1	PP reference	84
8.2	PP refinement	84
8.3	PP additions	86
8.3.1	Assets refinement	86
8.3.2	Additional assumptions	86
8.3.3	Additional Organization Security Policy	86
8.3.4	Additional threats	86
8.3.5	Additional security objectives	87
8.3.6	Additional security functional requirements	87
8.3.7	Additional assurance requirements from PP/9911	87
9	<i>RATIONALE</i>	87
9.1	Security objectives rationale	87
9.1.1	Assumptions addressed by objectives	88
9.1.2	Threats and security objectives	88

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 5/99


9.1.3	Organizational Security Policy addressed by objectives	88
9.2	Security requirements rationale	88
9.2.1	Security Functional Requirement rationale	88
9.2.2	Security functional requirements dependencies	89
9.2.3	Security assurance requirements	89
9.3	TOE summary specification rationale	89
9.4	PP claims rationale	90
10	<i>Glossary</i>.....	90
11	<i>Abbreviations</i>.....	95
12	<i>References</i>.....	98
12.1	TOE references	98
12.2	External documents references.....	98
12.3	Internal documents references.....	99

LIST OF FIGURES

Figure 1:	Smart card IC with Embedded Software	7
Figure 2 :	Embedded Software description.....	8
Figure 3 :	EMV Transaction flow.....	11
Figure 4 :	Smart card product life cycle.....	15

LIST OF TABLES

Table 1:	TOE limits	18
Table 2 :	Relationship between phases and threats	28
Table 3 :	Mapping of the security mechanisms and the IT security functions for EMV application	79
Table 4 :	Mapping of the security mechanisms and the IT security functions for B0' application	83
Table 5 :	Statement of assurance measures	84
Table 6 :	Mapping of the performed operations and the IT security functional requirements	85

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 6/99

1 ST INTRODUCTION

1.1 ST identification

<u>Title:</u>	Gem CB-B0'/EMV Security Target.
<u>Version:</u>	Public
<u>TOE :</u>	Gem CB-B0'/EMV
<u>TOE version:</u>	MPH021
<u>Product:</u>	Gem CB-B0'/EMV
<u>IT Security Evaluation & Certification scheme:</u>	French Scheme
<u>Integrated Circuit Certification reference :</u>	BSI-DSZ-CC-0170

This ST has been built with CC Version 2.1 and follows the French IT Security Evaluation and Certification Scheme:
The software reference and versions of this ST are defined in section 12.

1.2 ST overview

Smart Cards are being widely used in France for Debit/credit banking application. The GIE-CB (GIE-CB stands for the French central organization for banking cards) decided to migrate from the French banking application B0', to the EMV (Europay-MasterCard-Visa) standard. A solution to help this migration, stands in a new product which particular features are:


- VIS 1.3.2 compliance which allows the use of new banking mechanisms to enhance card management system.
- Proprietary French banking application (B0' V3) embedded in this product , co-existing with EMV application, that will help French banks through their EMV migration, ensuring a backward compatibility with their current terminals.

This new product is a Smart Card Integrated Circuit with a Gemplus Embedded Software that meets EMV standards (Europay-Master-Card-Visa), VIS (Visa Integrated Circuit Specification) and B0' requirements,

The aim of this document is to describe the Security Target (ST) of this new French EMV banking card GemCB-B0'/EMV product.

The main objectives of this ST are:

- to describe the Target-Of-Evaluation (TOE) ,the product type, the TOE environment and life-cycle, and to define the limits of the TOE ;
- to describe the security environment of the TOE, the assets to be protected and the threats to be countered by the TOE itself and by the environment during the development and the operational phases of the smart card.
- to describe the security objectives for the TOE and for its environment,
- to describe the security requirements which include the TOE security functional requirements and the TOE security assurance measures.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 7/99

1.3 CC conformance claim

This Security target is CC Part2 conformant and CC Part3 augmented.

This ST claims the PP “Smart Card Integrated Circuit With Embedded Software” Protection Profile version V2.0 reference PP/9911 issued June 1999.

This TOE relies on a Trusted IT product whose Security is compliant with PP9806.

As a consequence of PP/9911 claim, the PP/9806 is also claimed by including compliant IC Security Target to define IC security functions used by the TOE.

The Assurance level is EAL4 augmented. The minimum strength level for the Toe security functions is “SOF high” (Strength of functions high).

2 TOE DESCRIPTION

2.1 Product type

As shown in Figure 1, the TOE is the smart card Integrated Circuit with embedded software.

The software is a Debit/Credit banking application developed by Gemplus. It is embedded in an integrated circuit. (See product references in section 12).

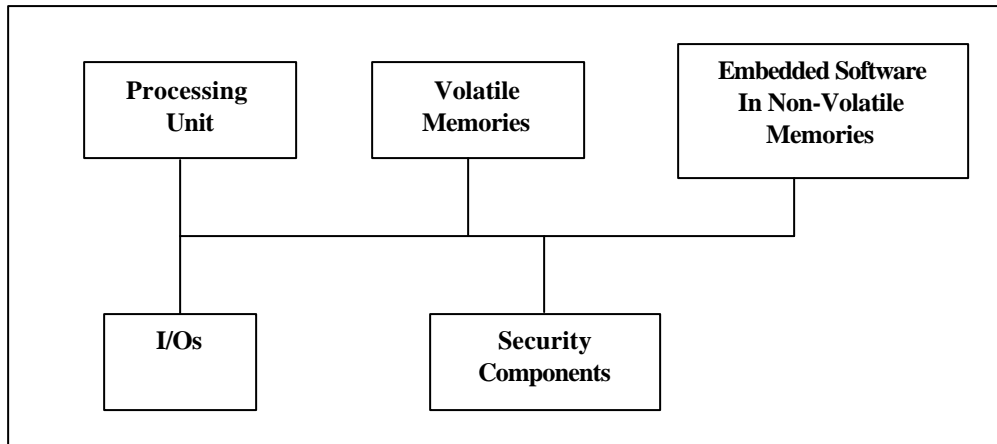


Figure 1: Smart card IC with Embedded Software


As required in the PP/9911, this security target addresses the requirement of the Embedded Software (ES).

The IC which is used to support the ES, is described in the Security Target referenced in section 12.2.

The ES is composed of the Basic Software (BS) and the Application Software (AS).

This AS contains two banking applications that meet the specifications stated in “Cahier des charges Technique du produit communautaire CB_B0'/EMV”.

- The CB-EMV application is compliant to the Europay-Mastercard-Visa specification, EMV'96 Integrated Circuit Card Specification for Payment Systems, release 3.1.1, May 31 1998,

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 8/99

- The B0' application is compliant to the "CB" B4-B0' V3 specification from Groupement des cartes bancaires, described in "specification technique et fonctionelle du masque B4 B0' V3, release 3.0 , June 20 2000.

Further in this document, the CB-EMV application is also called "EMV application ".

Figure 2 describes shortly how the TOE both applications EMV and B0' are implemented on the IC.

During personalization phase, the TOE may be personalized with both EMV and B0' personalization data, or with only EMV personalization data, or with only B0' personalization data. Thus, depending on personalization phase (which is out of the scope of this ST scope), the TOE may be used with both EMV or B0' terminals, or EMV terminals only, or B0' terminals only.

Basic software contains drivers used by both applications for communication with the IC. The Basic software includes also the start-up management that will start one application or the other, after chip reset.

The next sections presents EMV and B0' banking applications main features.

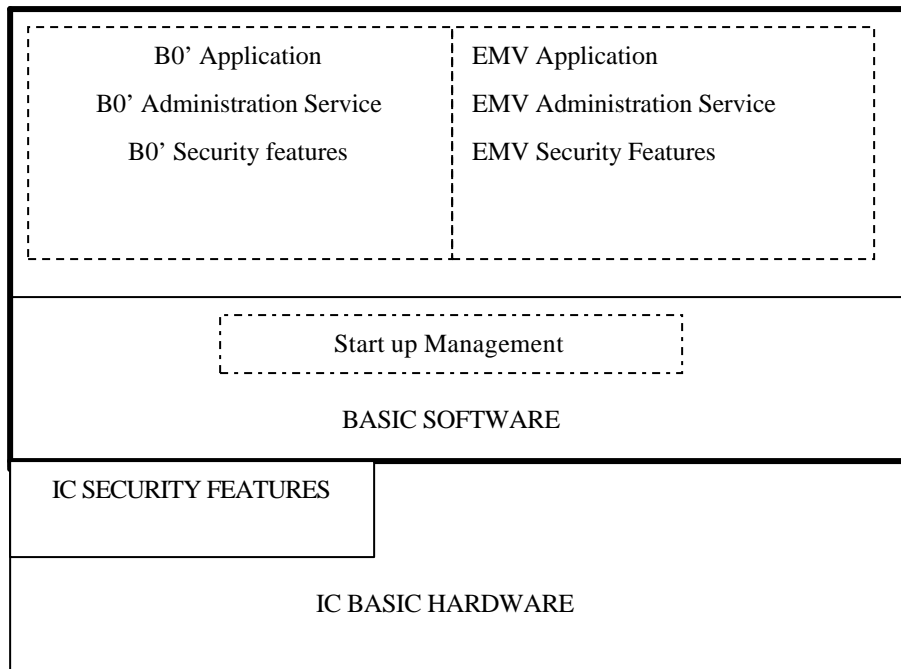

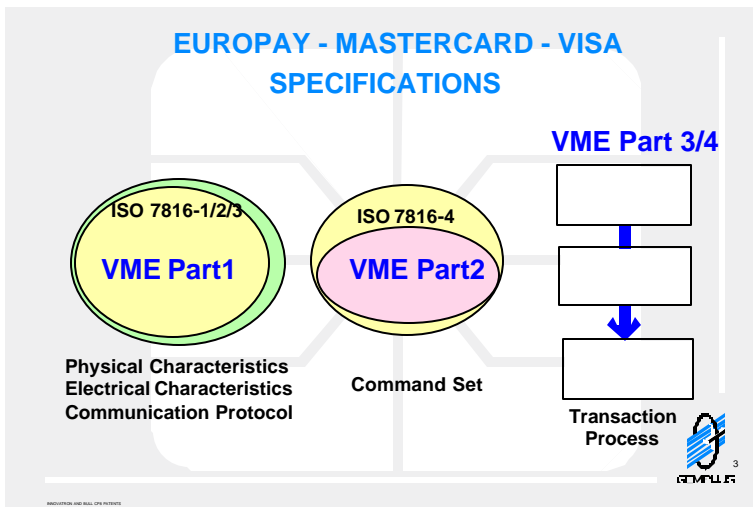
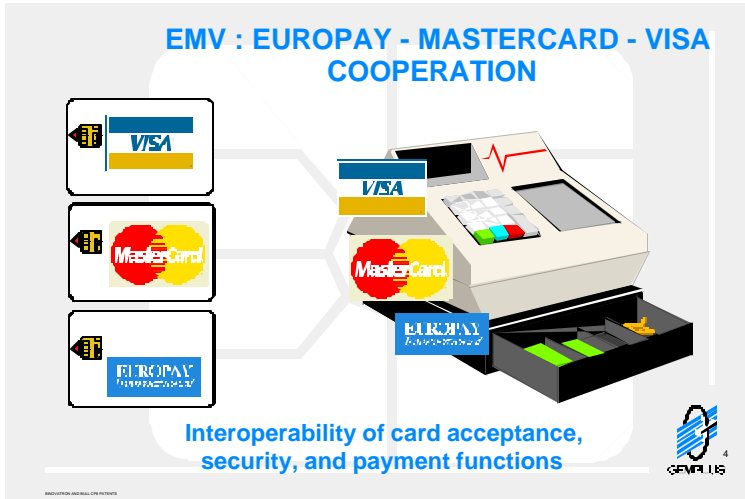


Figure 2 : Embedded Software description

2.1.1 EMV SPECIFICATIONS

The EMV 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).

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 9/99



EMV is based on ISO 7816 standards.


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.

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:

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 10/99

- 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 for signature.
- 6) the card will sign the payment with a certificate.

The **Figure 3** shows the EMV transaction flow extracted from VISA VIS 1.2.3 specification.

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.

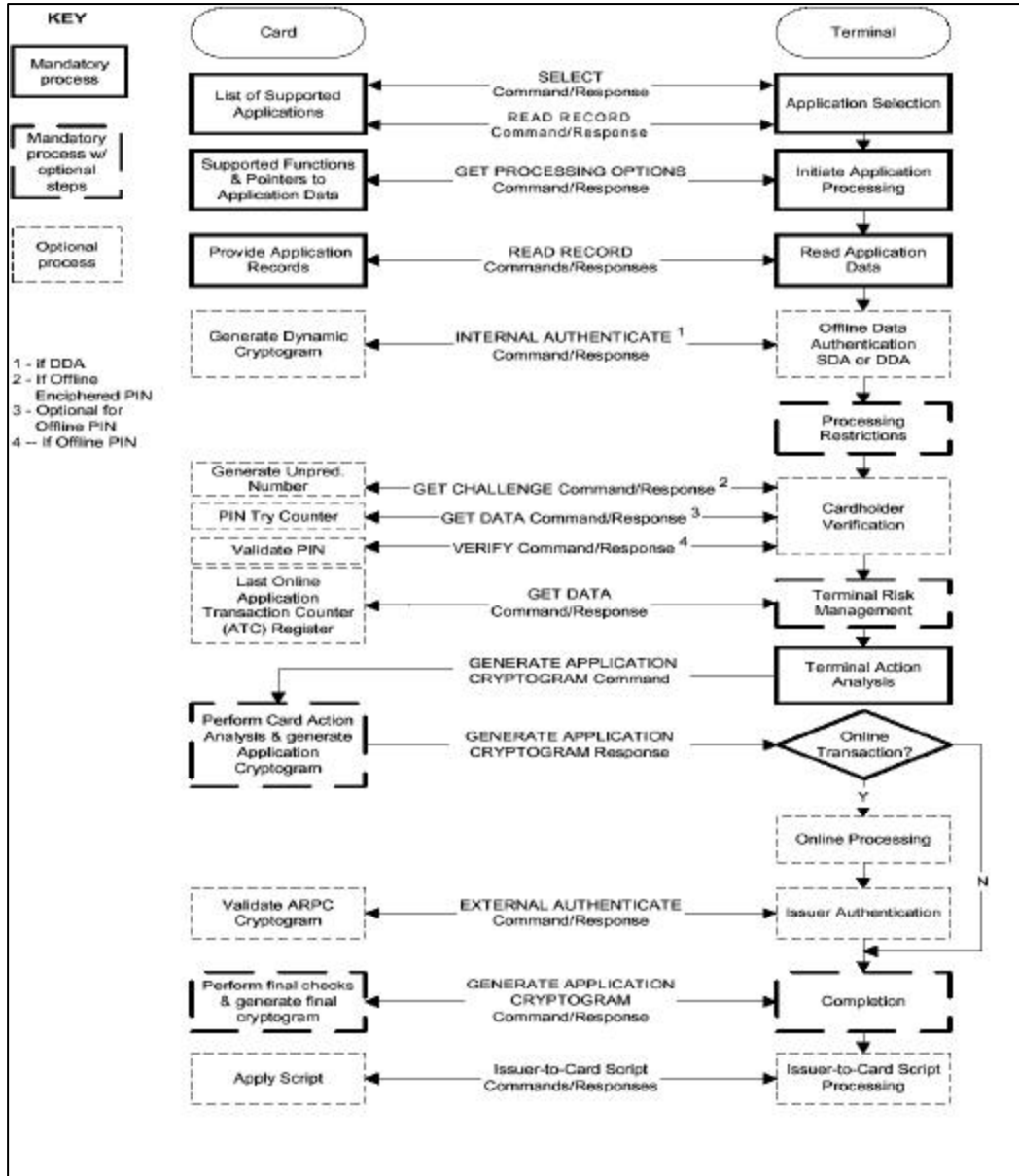



Figure 3 : EMV Transaction flow

Note : For this CB-EMV application , option 1 and 2 are not implemented. Offline data authentication is Static Data Authentication.

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


	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 12/99

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.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 13/99

2.1.2 B0' SPECIFICATION

B0' is the French banking application standard compliant with ISO 7816-3.

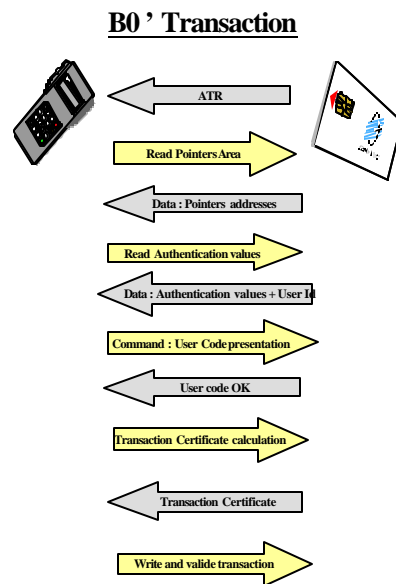
As the EMV standard, B0' aim is to ensure interoperability between credit cards and Point Of Sales or Automated Teller Machines.

Unlike EMV, very little management is left to the credit card itself. The Credit Card contains information that is checked by the terminal, and transaction decision is left to the Terminal.

Terminal sends commands to the card . The card executes the command and returns an execution status (Status Word) that indicates if the command was successful or not.


According to this execution status Terminal decides to continue the ongoing transaction or to abort it.

A typical card transaction is described below.



When a card is inserted in the terminal:

1. A Reset is applied to the card and the card sends back the **Answer To Reset (ATR)** that contains B0' application information like:
 - B0' life cycle phase.
 - Status word : state of the B0' application.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 14/99

2. If the card is not invalidated or blocked the Terminal will **read the card pointers area** to get information on the card memory area organization .
3. The card sends back the **memory mapping data**.
4. Then Terminal proceeds to card authentication and sends a command to **read the Authentication Values** contained in the card itself (VA : Valeur d'authentification + VS : Valeur d'authentification Statique),
5. Card sends back to Terminal these **Authentication values** with other possible data like End-User identity,
6. Terminal will verify if the Card Authentication values are correct, then ask **the End-User to authenticate itself** by entering his personal code (Personal Identifier Number),
7. The card will proceed to the verification of the End-User code and **return this verification result** to the Terminal.
8. If End-User authentication is correct , Terminal will proceed to the required transaction (payment, cash retrieval ..) and then ask the card to calculate the **transaction certificate** and send back the certification result,
9. The card returns the **certificate of the transaction** to the terminal,
10. Then the Terminal **writes the transaction** into the card and proceed to the **write validation**.


The data used by the Terminal for authentication (VA,VS), as well as certification secret keys, bank keys and Users Codes are stored in the card during personalization.

The card contains also data related to the maximum amount the End-User is allowed to spend during a given period (usually a one month period).

For each transaction, the Terminal will control if this maximum amount is reached. If so, the Terminal will require an authorization to the bank Terminal before processing the transaction.

B0' standard offers the possibility to automatically erase the transaction area.

In order to keep a registration of the automatic erasure, the B0' application will generate a 'dummy' maximum amount , forcing the Terminal to make an on-line call to the bank.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 15/99

2.2 Smart card product life cycle

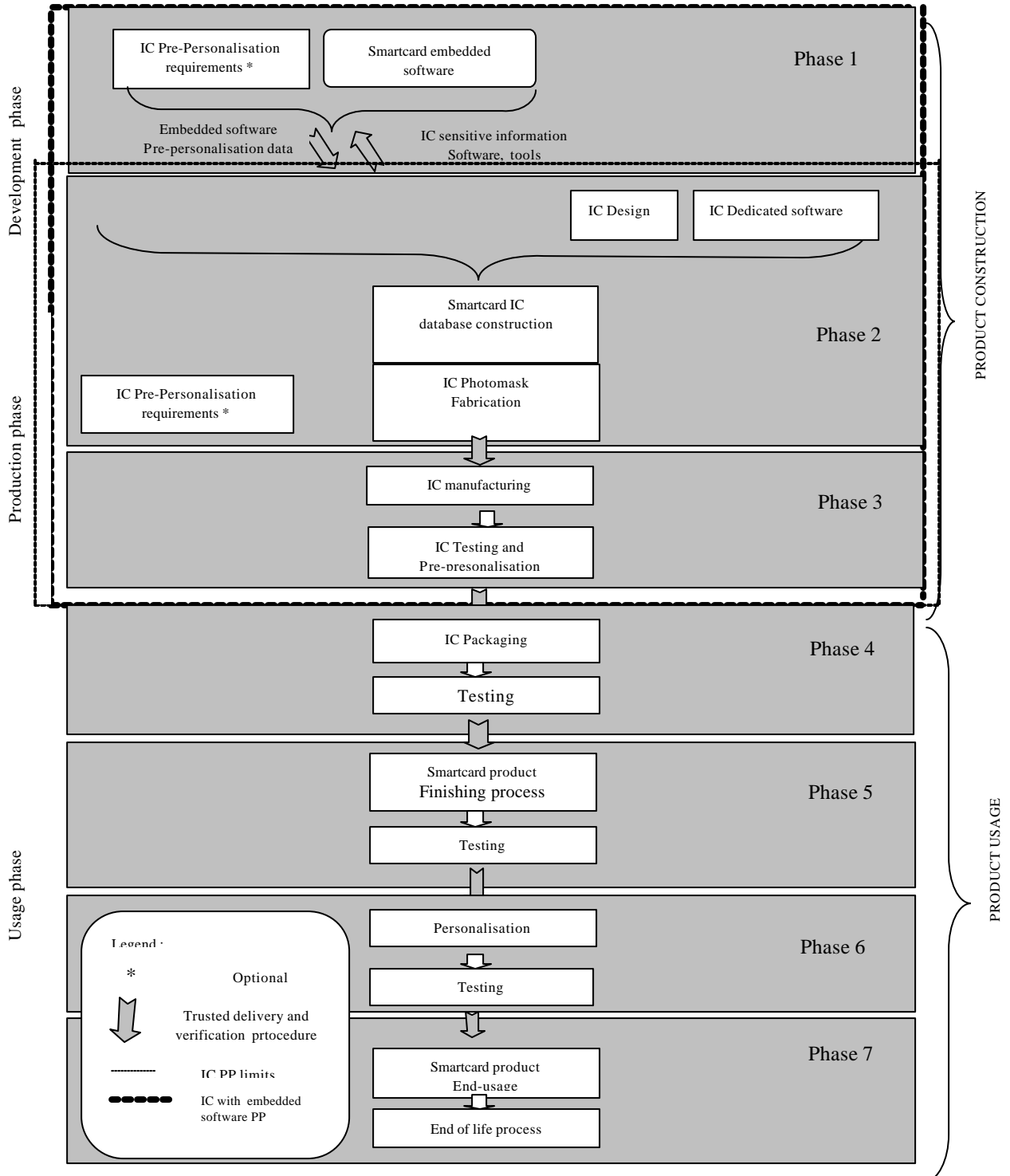



Figure 4 : Smart card product life cycle

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 16/99

2.2.1 THE TOE ACTORS

The banking application involves several actors along the TOE life-cycle:

2.2.1.1 *Payment organization*

The payment organization is a company which members are banks; the aim of this organization is to ensure interoperability among banks worldwide. For this product, the “Gie Carte Bancaire ” is the payment organization.

Gie CB:

- 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 banking application.

2.2.1.2 *Card issuer*

The card issuer -short named “issuer ”- is a bank which is a member of the Gie CB . 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 the personalization, the distribution and the invalidation of the cards it issues.

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

2.2.1.3 *The product developer*

The developer designs the chip ES during phase 1. For this product , the product developer is Gemplus at Gemenos site..

2.2.1.4 *The silicon manufacturer*

The silicon manufacturer -or founder- designs the IC during phase 2 and manufactures the Smartcard IC with the Embedded Software during phase 3.

For this product, the silicon manufacturer is Philips.


2.2.1.5 *The card manufacturer*

The card manufacturer is responsible for manufacturing Smartcards that is IC packaging and testing during phase 4 and Smart Card product finishing process and testing during phase 5 . For this product, the card manufacturer is Gemplus.

2.2.1.6 *The personalizers*

The personalizers personalize the card by loading the card issuer and Card-Holder data as well as application secrets such as cryptographic keys and PIN during phase 6.

As the TOE supports two different banking applications, the Smartcard will go through two different personalization processes that might be executed in different personalization sites. Therefore there will be two personalization guidance document, one for each application.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 17/99

The TOE may also be personalized in order to support only EMV transaction, or only B0' transaction.

2.2.1.7 The Card-Holder

The Card-Holder is a customer of the Card-Issuer. The card is personalized with the Card-Holder identification and secrets. The Card-Holder uses its personalized card during phase 7. It is also called the End-User.

2.2.1.8 The Service-Provider

The Service-Provider is the merchant or any organization that provides services during the card usage in phase 7.


2.2.1.9 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 be paid by the acquirer.

2.2.2 TOE ACTORS AND ROLES

The table below summarizes the actors and roles which have direct interface to the TOE or participate to the TOE construction .

Actors	Roles	Description
Product developer	Administrator	Develop the Embedded Software (AS and BS) in phase 1
Silicon manufacturer	Administrator	Design the IC during phase 2 and manufacture the IC during phase 3.
Card Manufacturer	Administrator	Manufacture IC with embedded software and set device to Initial state after IC masking.
Packaging manufacturer	Administrator	Set the card into creation state, may create basic file or basic memory structures.
Personalizer	Administrator	Create or load application data and put the card into operational state.
Card-Issuer	Administrator	Issues the card to the End-User. May decide to put the card into Termination state in phase 7.
Card-Holder (End-User)	User	Use the application loaded on the card
Terminals (ATM,POS)	User	Communicate with the card , executes commands and transactions

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 18/99

2.2.3 THE LIMITS OF THE TOE

Phase	Limit of the TOE	Industrial Step	Industrial Step Deliverables	Logical Phase EMV'	Logical Phase B0'	TOE main administrator	TOE users	Construction	PP 9806	PP 9911
1	Construction	Design	Software			Product Developer		Gemplus		X
2	Construction	Design	Hard mask set			Silicon Manufacturer		Philips	X	X
3	Construction	Production	Wafers with Chips.	Chip Initialization	Chip Initialization	Silicon Manufacturer		Philips	X	X
4	Usage	Production	Modules			Card Manufacturer	Module Manufacturing Process			
5	Usage	Production	Card with embedded module.	EMV Initialization		Packaging manufacturer	Card Initialization system and process			
6	Usage	Personalization	Card personalized	EMV Personalization	B0' Personalization	Card Personalizer	Card Personalization system and process			
7	Usage	Application (End Usage)		Usage	Usage CC1 Usage CC2	Card-Issuer	Card-Holder, Service Provider Card Issuer Terminals			

Table 1: TOE limits


The limit of the TOE is defined in the PP/9911, and corresponds to the development phase(phase 1 and 2)and production phase 3 of the smart card life-cycle.

The different logical phases are described in section 2.4

2.3 TOE environment

The TOE environment is defined as follows :

- Development environment corresponding to phase 1 and 2,
- Development and IC Photo-mask Fabrication environment corresponding to phases 2 addressed by the Smart Card IC PP,[PP/9806]
- IC manufacturing environment corresponding to phase 3, including the integration of the ES in the IC and the test operations,
- IC Packaging, Smart Card Finishing process environment corresponding to phases 4 and 5, including test operations,
- Personalization environment corresponding to personalization and testing of the Smart Card with the user data

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 19/99

- (phase 6),
- End-User environment (phase 7).

2.3.1 TOE DEVELOPMENT ENVIRONMENT

2.3.1.1 *Embedded Software development environment*

To assure security, the environment in which the development takes place must be made secure with controllable accesses having traceability. Furthermore, it is important that all authorized personnel involved fully understand the importance and the rigid implementation of defined security procedures.

The development begins with the TOE's specification. All parties in contact with sensitive information are required to abide by Non-Disclosure Agreements.

Design and development of the ES then follows. The engineer uses a secure computer system (preventing unauthorized access) to make his design, implementation and test performances.

Sensitive documents, databases on tapes, disks and diskettes are stored in an appropriately locked cupboard/safe. Also of paramount importance is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

Testing, programming and deliveries of the TOEs then take place. When these are done off-site, they must be transported and worked in a secure environment with accountability and traceability of all (good and bad) products.

During the transfer of sensitive data electronically, procedures must be established to ensure that the data arrives only at the destination and is not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies).

2.3.1.2 *IC development environment*

The IC development environment is defined in Smart Card PP/9806 and the IC Security Target referenced in section 12.

2.3.2 TOE PRODUCTION ENVIRONMENT

The production environment is defined in Smart Card PP/9806 and the IC Security Target referenced in section 12.

2.3.3 TOE USER ENVIRONMENT


Phases 4 and 5:

During phase 4 and 5 of production, the TOEs are used in the IC packaging, Smart Card Finishing process and the test environments. Everyone involved in such operations shall fully understand the importance of security procedures.

Moreover the environment in which these operations take place must be secured. Sensitive information (tape, disks or diskettes) are stored in an appropriately locked cupboard/safe. Also of paramount importance is the disposal of unwanted data (complete electronic erasures) and documents (i.e shredding).

Phase 6:

Since it is commonplace to produce high volumes of Smart Cards, adequate control procedures are necessary to account for all products at all stages.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 20/99

These must be transported and manipulated in a secure environment with accountability and traceability of all(good and bad) products.

Phase 7:

At the end of phase 6, the Card-Issuer delivers the Smart Card to the Card-Holder. The product being a banking debit/credit Card, the Card-Holder will use his Card for payment in shops through payment terminals), Point-Of-Sales terminal (POS), vending machines, or get cash through cash dispensers (Automatic Teller Machines).

In order to execute these operations in a safe way, the following steps shall be respected when the card is presented to the terminal :

- Identification of Card-Holder,
- Flow control regarding risk management (transaction amount, maximum transaction amount within a period..)
- Transaction certification
- During the usage phase the Card-Issuer (the bank) will be able to execute some operation on specific “Banking Machines” . Depending on the application type (EMV or B0’) these operations are i.e replacement of PIN code , changing maximum transaction amount, unblocking of blocked Cards.

2.4 TOE logical phases

During its construction usage, the TOE is under several logical phases as shown in Table 1. These phases are stored under a logical controlled sequence. The change from one phase to the next is under the TOE control.

- Chip initialization :

Chip initialization logical phase is set by the IC manufacturer and allows the use of the IC_key . This key is used for transportation protection between silicon manufacturer and card manufacturers in phase 4 . For this TOE , there are 2 IC keys loaded, one for the CB-EMV application , and another one for the B0’ application.

For the CB-EMV application , the IC_key is needed to test the produced modules in phase 4 and initialize the card during phase 5. At the end of phase 4, the CB-EMV module logical state is changed to Card initialization.

For the B0’ application, this IC_key is used until the end of phase 6. The Chip initialization state is not changed before end of phase 6.

Note that at the Chip Initialization stage, the IC manufacturer will load both IC_Keys, one for CB-EMV and one for B0’, whatever the Card Initialization process will be: Card Initialization with CB-EMV data alone, or with B0’ data alone, or for both applications.

- Card initialization :

For the CB-EMV application, the card initialization state is set at the end of phase 4. This state will allow the loading of pre-personalization data including personalization Secret keys, during phase 5.


If the card is to be personalized with EMV data only, the Card Initialization step will invalidate the use of B0’.

If Card is to be personalized with B0’ data only, card Initialization step will lock the EMV data and file creation, making the EMV application unusable.

- Card personalization :

For the CB-EMV application 6 the Card is personalization state is set at the end of phase 5. It allows the use of personalization Secret keys in phase 6.

- Usage :

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 21/99

For CB-EMV application, usage phase is set at the end of phase 6. It disables the previous phase and enables the use of the Smart card by the card holder.

- Usage phase 1 :


For the B0' application, usage phase 1 is set at the end of phase 6. It disables the previous phase and enables the use of the Smart card by the card holder with his Confidential code : CC1

- Usage phase 2 :

For the B0' application, usage phase may be set during usage phase 1 when Confidential Code is changed to CC2. It disables the previous phase and enables the use of the Smart card by the card holder with his Confidential code : CC2

2.5 TOE intended usage

As described in previous chapter, the TOE is dedicated to debit/credit banking application and is aimed to ensure interoperability both with EMV and B0' standards.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 22/99

3 TOE SECURITY ENVIRONMENT

This section describes the security aspects of the environment in which the TOE is intended to be used and addresses the description of the assets to be protected, the threats, the organizational security policies and the assumptions

In this section parts which are directly derived from PP/9911, are in italic characters.

3.1 Assets

As defined in the PP/9911, *assets are security relevant elements of the TOE that include :*

- *The IC specifications, design, development tools and technology,*
- *The IC Dedicated Software,*
- *The Smart Card Embedded Software including specifications, implementation and related documentation,*
- *The application data of the TOE (such as IC and system specific data, Initialization data, IC pre-personalization requirements and personalization data).*

The TOE itself is therefore an asset.

Assets have to be protected in terms of confidentiality and integrity.

PP9911 Assets refinement :

In this security target and for clarification purpose, assets defined as Application Data of the TOE are refined.

Application Data of the TOE include :


- Secret data like secret keys and Pin codes that have to be protected in terms of confidentiality and integrity.
- Transaction Specific Data used by the TOE to perform its security function during an CB-EMV transaction . The Transaction Specific Data is to be protected in integrity.

3.2 Assumptions

Security always concerns the whole system : the weakest element of the chain determines the total system security. *Assumptions described hereafter have to be considered for a secure system using Smart Card products .*

3.2.1 ASSUMPTIONS ON PHASE 1

<i>Assumption name</i>	<i>Description</i>
A.DEV_ORG*	<i>Procedures dealing with physical, personnel, organizational, technical measures for the confidentiality and integrity of Smart Card Embedded Software (e.g. source code and any associated documents) and IC designer proprietary information (tools, software, documentation...) shall exist and be applied in software development.</i>

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 23/99

3.2.2 ASSUMPTIONS ON THE TOE DELIVERY PROCESS (PHASE 4 TO 7)

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives as described in the following assumptions.


<i>Assumption name</i>	<i>Description</i>
A.DLV_PROTECT*	<i>Procedures shall ensure protection of TOE material/information under delivery and storage.</i>
A.DLV_AUDIT*	<i>Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.</i>
A.DLV_RESP*	<i>Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.</i>

3.2.3 ASSUMPTIONS ON PHASES 4 TO 6

<i>Assumption name</i>	<i>Description</i>
A.USE_TEST*	<i>It is assumed that appropriate functionality testing of the IC is used in phases 4, 5 and 6.</i>
A.USE_PROD*	<i>It is assumed that security procedures are used during all manufacturing and test operations through phases 4, 5, 6 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).</i> Refinement : specific security recommendations are to be followed: <ul style="list-style-type: none"> - Card must have a unique personalization identification , and personalization must be operated with a process that prevents from fraudulent or unexpected cloning.

3.2.4 ASSUMPTIONS ON PHASE 7

<i>Assumption name</i>	<i>Description</i>
A.USE_DIAG*	<i>It is assumed that secure communication protocols and procedures are used between Smart Card and terminal.</i> Refinement : specific security recommendations are to be followed: <ul style="list-style-type: none"> - The end-user is the only actor to know the PIN in a deciphered way. - PIN code mailing must be separated from the card mailing. - A card must never be close to any document giving PIN contents - The card administrator servers must keep the all application secret keys with a high level of confidentiality. - The transaction contents must be archived in case of repudiation or any other dispute. - The off-line transactions signatures must be audited.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 24/99

--	--

3.3 Threats

The TOE as defined in chapter 2 is required to counter the threats described hereafter, a threat agent wishes to abuse the assets either by functional attacks or by environmental manipulation, by specific hardware manipulation, by a combination of hardware and software manipulations or by any other type of attacks.

Threats have to be split in:

- threats against which specific protection within the TOE is required (class I),
- threats against which specific protection within the environment is required (class II).

3.3.1 UNAUTHORIZED FULL OR PARTIAL CLONING OF THE TOE

Threat name	Description
<i>T.CLON*</i>	<i>Functional cloning of the TOE (full or partial) appears to be relevant to all phases of the TOE life-cycle, from phase 1 to phase 7, but only phases 1 and 4 to 7 are considered here, since functional cloning in phases 2 and 3 are purely in the scope of Smart Card IC PP. Generally, this threat is derived from specific threats combining unauthorized disclosure, modification or theft of assets at different phases.</i>

3.3.2 THREATS ON PHASE 1


During phase 1, three types of threats have to be considered:

- a) *threats on the Smart Card Embedded Software and its development environment, such as: unauthorized disclosure, modification or theft of the Smart Card Embedded Software and/or initialization data at phase 1;*
- b) *threats on the assets transmitted from the IC designer to the Smart Card software developer during the Smart Card ES development;*
- c) *threats on the Smart Card Embedded Software and initialization data transmitted during the delivery process from the Smart Card Embedded Software developer to the IC designer.*

Unauthorized disclosure of assets

This type of threats covers unauthorized disclosure of assets by attackers who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.

Threat name	Description
<i>T.DIS_INFO*</i> (type b)	<i>Unauthorized disclosure of the assets delivered by the IC designer to the Smart Card Embedded Software developer such as sensitive information on IC specification, design and technology, software and tools if applicable.</i>
<i>T.DIS_DEL*(type c)</i>	<i>Unauthorized disclosure of the Smart Card Embedded Software and any additional application data (such as IC pre-personalization requirements) during the delivery process to the IC designer.</i>

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 25/99

<i>T.DIS_ES1</i> (type a)	<i>Unauthorized disclosure of ES (technical or detailed specifications, implementation code) and/or Application Data(such as secrets, or control parameters for protection system, specification and implementation for security mechanisms).</i>
<i>T.DIS_TEST_ES</i> (type a and c)	<i>Unauthorized disclosure of the Smart Card ES test programs or any related information.</i>

Theft or unauthorized use of assets

Potential attackers may gain access to the TOE and perform operations for which they are not authorized. For example, such an attacker may personalize, modify or influence the product in order to gain access to the Smart Card application system.

Threat name	Description
<i>T.T_DEL</i> *(type c)	<i>Theft of the Smart Card Embedded Software and any additional application data (such as pre-personalization requirements) during the delivery process to the IC designer.</i>
<i>T.T_TOOLS</i> (type a and b)	<i>T.T_TOOLS(a and b) Theft or unauthorized use of the Smart Card ES development tools (such as PC, development software, data bases).</i>
<i>T.T_SAMPLE2</i> (type a)	<i>Theft or unauthorized use of TOE samples (e.g. bond-out chips with Embedded Software).</i>

Unauthorized modification of assets


The TOE may be subjected to different types of logical or physical attacks which may compromise the security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security may be bypassed or compromised reducing the integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threats includes the implementations of Trojan horses.

Threat name	Description
<i>T.MOD_DEL</i> * (type c)	<i>Unauthorized modification of the Smart Card Embedded Software and any additional application data (such as IC pre-personalization requirements) during the delivery process to the IC designer.</i>
<i>T.MOD</i> (type a)	<i>Unauthorized modification of ES and/or Application Data or any related information (technical specifications).</i>

3.3.3 THREATS ON DELIVERY FOR/FROM PHASE 1 TO PHASE 4 TO 6

Threats on data transmitted during the delivery process from the Smart Card developer to the IC packaging manufacturer, the Finishing process manufacturer or the Personalizer.

These threats are described hereafter:

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 26/99

<i>Threat name</i>	<i>Description</i>
<i>T.DIS_DEL1</i>	<i>Unauthorized disclosure of Application Data during delivery to the IC packaging manufacturer, the Finishing process manufacturer or the Personalizer.</i>
<i>T.DIS_DEL2</i>	<i>Unauthorized disclosure of Application Data delivered to the IC packaging manufacturer, the Finishing process manufacturer or the Personalizer.</i>
<i>T.MOD_DEL1</i>	<i>Unauthorized modification of Application Data during delivery to the IC packaging manufacturer, the Finishing process manufacturer or the Personalizer.</i>
<i>T.MOD_DEL2</i>	<i>Unauthorized modification of Application Data delivered to the IC packaging manufacturer, the Finishing process manufacturer or the Personalizer.</i>

3.3.4 THREATS ON PHASES 4 TO 7

During these phases, the assumed threats could be described in three types:

- Unauthorized disclosure of assets,
- Theft or unauthorized use of assets,
- Unauthorized modification of assets.

Unauthorized disclosure of assets

This type of threats covers unauthorized disclosure of assets by attackers who may possess a wide range of technical skills, resources and motivation. Such attackers may also have technical awareness of the product.

<i>Threat name</i>	<i>Description</i>
<i>T.DIS_ES2</i>	<i>Unauthorized disclosure of ES and Application Data (such as data protection systems, memory partitioning, cryptographic programs and keys).</i>


Theft or unauthorized use of assets

Potential attackers may gain access to the TOE and perform operations for which they are not allowed. For example, such attackers may personalize the product in an unauthorized manner, or try to gain fraudulently access to the Smart Card system.

<i>Threat name</i>	<i>Description</i>
<i>T.T_ES</i>	<i>Theft or unauthorized use of TOE silicon samples (e.g. bond out chips with embedded software).</i>
<i>T.T_CMD</i>	<i>Unauthorized use of instructions or commands or sequence of commands sent to the TOE.</i>

Unauthorized modification of assets

The TOE may be subjected to different types of logical or physical attacks which may compromise security. Due to the intended usage of the TOE (the TOE environment may be hostile), the TOE security parts may be bypassed or

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 27/99

compromised reducing the integrity of the TOE security mechanisms and disabling their ability to manage the TOE security. This type of threats includes the implementation of malicious Trojan horses, Trapdoors, downloading of viruses or unauthorized programs.

<i>Threat name</i>	<i>Description</i>
<i>T.MOD_LOAD</i>	<i>Unauthorized loading of programs.</i>
<i>T.MOD_EXE</i>	<i>Unauthorized execution of programs.</i>
<i>T.MOD_SHARE</i>	<i>Unauthorized modification of program behaviour by interaction of different programs.</i>
<i>T.MOD_SOFT*</i>	<i>Unauthorized modification of Smart Card Embedded Software and Application Data.</i>

Additional threats to PP9911

Following threats have been added to fulfill specific **CB-EMV** security requirements during phase 7


Threat name	Description
T.MOD_TR_EMV	Unauthorized modification of Transaction Specific Data stored and used by the TOE during its function processing and during usage phase (phase 7) for CB-EMV application

The table given below indicates the relationship between the phases of the Smart Card life cycle, the threats and the type of the threats.

Threats have been split in :

- Threats against which specific protection within the TOE is required (class I),
- Threats against which specific protection within the environment is required (class II).

Threats	Phase1	Phase4	Phase5	Phase6	Phase7
<i>T.CLON*</i>	<i>Class II</i>	<i>Class I</i>	<i>Class I</i>	<i>Class I</i>	<i>Class I</i>
<i>T.DIS_INFO*</i>	<i>Class II</i>				
<i>T.DIS_DEL*</i>	<i>Class II</i>				
<i>T.DIS_DEL1</i>	<i>Class II</i>				
<i>T.DIS_DEL2</i>		<i>Class II</i>	<i>Class II</i>	<i>Class II</i>	
<i>T.DIS_ES1</i>	<i>Class II</i>				
<i>T.DIS_TEST_ES</i>	<i>Class II</i>				
<i>T.DIS_ES2</i>		<i>Class I</i>	<i>Class I</i>	<i>Class I</i>	<i>Class I</i>
<i>T.T_DEL*</i>	<i>Class II</i>				
<i>T.T_TOOLS</i>	<i>Class II</i>				
<i>T.T_SAMPLE2</i>	<i>Class II</i>				

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 28/99

<i>Threats</i>	<i>Phase1</i>	<i>Phase4</i>	<i>Phase5</i>	<i>Phase6</i>	<i>Phase7</i>
<i>T.T_ES</i>		<i>Class I</i>	<i>Class I</i>	<i>Class I</i>	<i>Class I</i>
<i>T.T_CMD</i>		<i>Class I</i>	<i>Class I</i>	<i>Class I</i>	<i>Class I</i>
<i>T.MOD_DEL*</i>	<i>Class II</i>				
<i>T.MOD_DEL1</i>	<i>Class II</i>				
<i>T.MOD_DEL2</i>		<i>Class II</i>	<i>Class II</i>	<i>Class II</i>	
<i>T.MOD</i>	<i>Class II</i>				
<i>T.MOD_SOFT*</i>		<i>Class I</i>	<i>Class I</i>	<i>Class I</i>	<i>Class I</i>
<i>T.MOD_LOAD</i>		<i>Class I</i>	<i>Class I</i>	<i>Class I</i>	<i>Class I</i>
<i>T.MOD_EXE</i>		<i>Class I</i>	<i>Class I</i>	<i>Class I</i>	<i>Class I</i>
<i>T.MOD_SHARE</i>		<i>Class I</i>	<i>Class I</i>	<i>Class I</i>	<i>Class I</i>
<i>T.MOD_TR_EMV</i>					<i>Class I</i>

Table 2 : Relationship between phases and threats

Note: Phases 2 and 3 are covered in the scope of Smart Card IC PP.


T.MOD_TR_EMV applies only to Transaction Specific Data stored and used by the TOE to perform its functions for CB-EMV application, and is therefore a Class I threat.

3.4 Organizational security policy

The organizational security policy involves statements or rules with which the TOE must comply.

The TOE policies stated in this ST are due to EMV and B0' standard and specifications referenced in chapter 12.

Organizational Security policy	Description
OSP.CB-EMV	TOE is designed to be conform to CB-EMV specifications (see reference in 12.2)
OSP.B0'	TOE is designed to be conform to B0' specifications (see reference in 12.2)
OSP.CRYPTO	TOE shall respect the French laws on the cryptographic usage. (see reference in 12.2)
OSP.REPUD_EMV	TOE contributes to the non-repudiation of a transaction processed by the TOE on behalf of the authorized card holder for CB-EMV application .
OSP.TOE_AUTH_EMV	TOE provides means to be authenticated by the IT remote system during phase 4 to 6 of CB-EMV application card manufacturing process.
OSP.TOE_LOGO	A mark allowing to identify the IC manufacturer is visible on the IC.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 29/99

4 TOE SECURITY OBJECTIVES


The security objectives of the TOE cover principally the following aspects:

- integrity and confidentiality of assets,
- protection of the TOE and associated documentation and environment during development and production phases.

4.1 TOE Security Objectives

The TOE shall use state of art technology to achieve the following IT security objectives, and for that purpose, when IC physical security features are used, the specification of those IC physical security features shall be respected. When IC physical security features are not used, the Security Objectives shall be achieved in other ways:

Sec. Obj. Name	Description
<i>O.TAMPER_ES</i>	<i>The TOE must prevent tampering with its security critical parts. Security mechanisms have especially to prevent the unauthorized change of functional parameters, security attributes and secrets such as the life cycle sequence flags and cryptographic keys. The ES must be designed to avoid interpretations of electrical signals from the hardware part of the TOE.</i>
<i>O.CLON*</i>	<i>The TOE functionality needs to be protected from cloning.</i>
<i>O.OPERATE*</i>	<i>The TOE must ensure the continued correct operation of its security functions.</i>
<i>O.FLAW*</i>	<i>The TOE must not contain flaws in design, implementation or operation.</i>
<i>O.DIS_MECHANISM2</i>	<i>The TOE shall ensure that the ES security mechanisms are protected against unauthorized disclosure.</i>
<i>O.DIS_MEMORY*</i>	<i>The TOE shall ensure that sensitive information stored in memories is protected against unauthorized disclosure.</i>
<i>O.MOD_MEMORY*</i>	<i>The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification.</i>
O.REPUD_EMV	The TOE shall contribute to the non-repudiation of a CB-EMV processed Transaction by the TOE on behalf of the authorized card holder for EMV application .
O.TOE_AUTH_EMV	The TOE shall provide means to be authenticated by the IT remote system during phase 4 to phase 6 of CB-EMV card manufacturing process.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 30/99


4.2 Environment Security objectives

4.2.1 OBJECTIVES ON PHASE 1

<i>Sec. Obj. Name</i>	<i>Description</i>
<i>O.DEV_TOOLS*</i>	<i>The Smart Card ES shall be designed in a secure manner, by using exclusively software development tools (compilers, assemblers, linkers, simulators etc...) and software-hardware integration testing tools (emulators) that will result the integrity of program and data.</i>
<i>O.DEV_DIS_ES</i>	<i>The Embedded Software developer shall use established procedures to control storage and usage of the classified development tools and documentation, suitable to maintain the integrity and the confidentiality of the assets of the TOE.</i> <i>It must be ensured that tools are only delivered to the parties authorized personnel. It must be ensured that confidential information on defined assets are only delivered to the parties authorized personnel on a need to know basis.</i>
<i>O.SOFT_DLV*</i>	<i>The Smart Card Embedded Software must be delivered from the Smart Card Embedded Software developer (Phase 1) to the IC designer through a trusted delivery and verification procedure that shall be able to maintain the integrity of the software and its confidentiality, if applicable.</i>
<i>O.INIT_ACS</i>	<i>Initialization Data shall be accessible only by authorized personnel (physical, personnel, organizational, technical procedures).</i>
<i>O.SAMPLE_ACS</i>	<i>Samples used to run tests shall be accessible only by authorized personnel.</i>
O.DEV_DIS_ES_SPEC	The Embedded Software developer shall use EMV and B0' standard to design the ES and respect the 'French laws on the cryptographic usage' when cryptographic calculation is used.

4.2.2 OBJECTIVES ON THE TOE DELIVERY PROCESS (PHASES 4 TO 7)

<i>Sec. Obj. Name</i>	<i>Description</i>
<i>O.DLV_PROTECT*</i>	<i>Procedures shall ensure protection of TOE material/information under delivery including the following objectives:</i> <ul style="list-style-type: none"> • non-disclosure of any security relevant information, • identification of the elements under delivery, • meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgement), • physical protection to prevent external damage, • secure storage and handling procedures (including rejected TOE's) • traceability of TOE during delivery including the following parameters:

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 31/99

	<ul style="list-style-type: none"> • <i>origin and shipment details,</i> • <i>reception, reception acknowledgement,</i> • <i>location material/information.</i>
<i>O.DLV_AUDIT*</i>	<i>Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process (including if applicable any non-conformance to the confidentiality convention) and highlight all non conformance to this process.</i>
<i>O.DLV_RESP*</i>	<i>Procedure shall ensure that people (shipping department, carrier, reception department) dealing with the procedure for delivery have got the required skill, training and knowledge to meet the procedure requirements and be able to act fully in accordance with the above expectations.</i>

4.2.3 OBJECTIVES ON DELIVERY FROM PHASE 1 TO PHASE 4, 5 AND 6


<i>Sec. Obj. Name</i>	<i>Description</i>
<i>O.DLV_DATA</i>	<i>The application Data must be delivered from the Smart Card Embedded Software developer (phase1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and confidentiality of the Application Data.</i>

4.2.4 OBJECTIVES ON PHASES 4 TO 6

<i>Sec. Obj. Name</i>	<i>Description</i>
<i>O.TEST_OPERATE*</i>	<p><i>Appropriate functionality testing of the IC shall be used in phases 4 to 6.</i></p> <p><i>During all manufacturing and test operations, security procedures shall be used through phases 4, 5, 6 to maintain confidentiality and integrity of the TOE and of its manufacturing and test data.</i></p> <p><u>Refinement</u> : specific security recommendations are to be followed:</p> <p>Card must have a unique personalization identification and personalization must be operated with a process that prevents from fraudulent or unexpected cloning.</p>

4.2.5 OBJECTIVES ON PHASE 7


<i>Sec. Obj. Name</i>	<i>Description</i>
<i>O.USE_DIAG*</i>	<i>Secure communication protocols and procedures shall be used between Smart Card and terminal.</i>

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 32/99

	<p><u>Refinement</u> : specific security recommendations are to be followed:</p> <ul style="list-style-type: none"> - The end-user is the only actor to know the PIN in a deciphered way. PIN code mailing must be separated from the card mailing. A card must never be close to any document giving PIN contents - The card administrator servers must keep the all application secret keys with a high level of confidentiality. - The transaction contents must be archived in case of repudiation or any other dispute. - The off-line transactions signatures must be audited.
--	---

4.2.6 ADDITIONAL OBJECTIVE FOR THE IC

<i>Sec. Obj. Name</i>	<i>Description</i>
O.TOE_LOGO	A mark allowing to identify the IC manufacturer shall be visible on the IC.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 33/99

5 TOE IT 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.

Due to the fact that after TOE startup, either the EMV application, either the B0' application will be launched, and that each application owns and manages its own security features, the TOE security function requirements is split in two different sections, one for each application.

5.1 TOE security functional requirements for EMV application

5.1.1 DEFINITION OF EMV SUBJECT, OBJECTS AND ATTRIBUTES


The following tables list Subjects , objects and security attributes, used in the EMV application security function description.

5.1.1.1 Subjects

Subjects	Description
SUB_CMDMAN_EMV	Process that receives and interpret the command messages sent by the remote IT product.
SUB_CMD_EMV	Process activated on SUB_CMDMAN_EMV request according to a specific command message. SUB_CMD_EMV is an object for SUB_CMDMAN_EMV. SUB_CMD_EMV performs operations on objects : OB_PIN, OB_AUTH_KEY_EMV, OB_DFILE, OB_EFILE, OB_APTLV. SUB_CMD_EMV is therefore a subject for the previous listed objects.
SUB_CRYPTALGO_EMV	Process performing cryptographic computation. SUB_CRYPTALGO_EMV is activated by a SUB_CMD_EMV Subjects.

5.1.1.2 Objects


Objects	Type	Description
OB_DFILE	User Data	Dedicated File: entity in EEPROM being part of the TOE_EMV file structure and containing other(s) objects OB_EFILE or OB_DFILE.
OB_EFILE	User Data/ TSF Data	Elementary File: entity in EEPROM being part of the TOE_EMV file structure and containing User or TSF data

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 34/99

Objects	Type	Description
OB_AUTH_KEY_EMV	User Data	Entity in EEPROM containing a cryptographic key used in authentication. .This includes: -IC_Key : loaded by Silicon manufacturer and used to authenticate card manufacturer, Authentication Keys loaded during initialization to authenticate Personalizer, -Authentication Keys loaded during personalization to authenticate administrator and user during usage phase. Authentication keys are stored in a OB_EFILE.
OB_KEY_EMV	TSF Data	Entity in EEPROM containing a other cryptographic used by the TSF to ensure it's security functions. This includes: -Key used for random number generation and loaded by Silicon manufacturer, -Keys loaded during initialization phase for integrity and confidentiality during personalization phase, -Keys loaded during personalization phase for integrity and confidentiality during usage phase. Keys used for integrity and confidentiality are stored in an OB_EFILE.
OB_PIN	User Data	Entity in EEPROM containing the PIN. Stored in a OB_EFILE .
OB_APTLV	User Data	Entity in EEPROM containing an Application Proprietary TLV Object data object . May be stored in an OB_EFILE.
OB_TRANS	User Data	Transaction Specific Data stored in an OB_EFILE .This object is part of OB_APTLV and is used by the TOE to generated the Application Cryptogram.
OB_RAM	TSF Data	Entity in RAM containing cryptographic variables used for cryptographic computation and data used for command processing.
OB_RND_SEED	TSF Data	Value used by TOE to generate random number .

5.1.1.3 Security attributes

Security Attributes	Description
Card Life Cycle Status	Indicates if card life status is : Issuer, User, disabled, blocked.
Command Life Cycle	Indicates if command is allowed according to card life status.
Command Header Format attributes	Command header attributes: contain class of instruction (CLA), instruction code (INS), and instruction parameters (mandatory parameters are P1, P2).
Command Key security attributes	Defines if a specific right shall be granted before executing the command.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 35/99


Security Attributes	Description
Card Security Status group	Contains : {Pin Security Status, Key Security Status, Secure Messaging Status}.
Command File Type	Indicates if a command may be executed according to file type.
File Type	File type : MF,DF,EF.
File Access Conditions	Access condition attached to each file indicates for a group of command if access authorized/not authorized, submitted to authentication , must use secure messaging. Values are : ALWAYS, NEVER, CHV,SMI,SMC, EXAU,APPLI
File Header LRC	File header Checksum used to check file structure integrity
Key Type	Indicates if key is to be used for : Secure Messaging for integrity, Secure Messaging for confidentiality, Application cryptogram, Issuer authenticate, External authenticate used in personalization.
Cryptographic Algorithm Type	Indicates if Algorithm is for : Secure Messaging for integrity, Secure Messaging for confidentiality, Application cryptogram, Issuer authenticate, External authenticate used in personalization
Key Checksum	Value stored with Key value, and used to check Key integrity.
PIN Checksum	PIN checksum stored with PIN and used to check PIN integrity.
Ratification group of security attributes	Contains : {Maximum Presentation Number, Ratification Counter}.
TLV Life cycle	Indicates if OB_TLV access is allowed or not.
TLV Read Access List	Indicates if OB_TLV reading is allowed or not.
TLV Update Access List	Indicates if OB_TLV updating is allowed or not.
TLVObject LRC	Application Proprietary TLV Checksum used to check OB_APTLV integrity. This LRC applies to specific TLV Objects dedicated to Card Risk Management including OB_TRANS object
Random seed Checksum	Value used to check the OB_RND_SEED integrity. This value is initialized when Random seed is loaded by Silicon manufacturer.
Application Block Flag	Application block Bit indicating if application (s) under OB_DFILE is (are) blocked.

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 :

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 36/99

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

1. **Card Life Cycle Status discrepancy;**
2. **EEPROM programming failure;**
3. **File structure integrity failure;**
4. **Application proprietary TLV object integrity;**
5. **Authentication data integrity failure;**
6. **Configuration integrity failure;**
7. **Random seed integrity error**

b) Other rule: **none.**

5.1.3 NON-REPUDIATION OF ORIGIN (FCO_NRO)

5.1.3.1 FCO_NRO.1 Selective proof of origin

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for **Transaction Specific Data** at the request of the **recipient, no third parties.**

FCO_NRO.1.2 The TSF shall be able to relate the **OB_AUTH_KEY_EMV** of the originator of the information , and the **OB_TRANS field** of the information to which the evidence applies.

FCO_NRO.1.3 The TSF shall provide a capability to verify the evidence of origin of information to **recipient, no third parties** given **no delay in response.**


Refinement : This requirement applies to on-line transaction for which immediate response is needed from recipient to complete the transaction process.

5.1.4 CRYPTOGRAPHIC KEY MANAGEMENT (FCS_CKM)

5.1.4.1 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1/RDR The TSF shall perform **cryptographic key transfer from EEPROM to RAM** in accordance with a specified cryptographic key access method, "**Transfer Method**" that meets the following standard : **none.**

FCS_CKM.3.1/UPT The TSF shall perform **cryptographic key transfer from RAM to EEPROM** in accordance with a specified cryptographic key access method "**Transfer Method**" that meets the following standard : **none.**

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 37/99

5.1.4.2 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**.

5.1.5 CRYPTOGRAPHIC OPERATIONS (FCS_COP)

5.1.5.1 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 1.3.2 (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 1.3.2 (Only in phase 7)**.


5.1.6 ACCESS CONTROL POLICY (FDP_ACC)

5.1.6.1 FDP_ACC.2 Complete access control

SFP : CMD_EMV/ EMV Command Access control

FDP_ACC.2.1/ CMD_EMV The TSF shall enforce the **EMV Command Access Control SFP** on the **subject SUB_CMDMAN_EMV** and **all the objects SUB_CMD_EMV**, and all operations among subjects and objects covered by the SFP.

Subjects	Objects	Operations among subjects and objects
SUB_CMDMAN_EMV	SUB_CMD_EMV	- activation of SUB_CMD_EMV by SUB_CMDMAN_EMV
General rules		

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 38/99

- Only SUB_CMDMAN_EMV can activate a SUB_CMD_EMV upon receipt of a command message;
 - SUB_CMD_EMV 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_EMV of administrator-reserved SUB_CMD_EMV;
- Refinement: Once the card initialization phase is completed, the TOE_EMV, does not allow the creation of SUB_CMD_EMV subjects

**FDP_ACC.2.2/
CMD_EMV** 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.

SFP : FILE_EMV / EMV File Access control SFP


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

Subjects	Objects	Operations among subjects and objects
SUB_CMD_EMV	OB_DFILE OB_EFILE	<ul style="list-style-type: none"> - creation of OB_EFILE or OB_DFILE stored in OB_DFILE by SUB_CMD_EMV; - creation, update and read of data element(s) stored in OB_EFILE by SUB_CMD_EMV;
General rules		
<ul style="list-style-type: none"> - SUB_CMD_EMV shall create OB_EFILE or OB_DFILE in OB_DFILE only if the access conditions of OB_DFILE are fulfilled; - SUB_CMD_EMV shall have access to data element(s) stored in OB_EFILE only if the access conditions of the file are fulfilled; <p><u>Refinement</u> : these operations concern data exchange with the current user of the TOE_EMV, not the TOE_EMV internal exchanges</p>		

**FDP_ACC.2.2/
FILE_EMV** 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.

SFP: SEC_EMV / EMV Secret Access Control

**FDP_ACC.2.1/
SEC_EMV** The TSF shall enforce the **EMV Secret Access Control SFP** on **all the subjects SUB_CRYPTALGO_EMV and SUB_CMD_EMV** and **all the objects OB_AUTH_KEY_EMV and OB_PIN**, and all operations among subjects and objects

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 39/99

covered by the SFP.


Subjects	Objects	Operations among subjects and objects
SUB_CRYPTALGO_E MV SUB_CMD_EMV	OB_AUTH_KEY_EMV OB_PIN	<ul style="list-style-type: none"> - read, update of OB_AUTH_KEY_EMV and OB_PIN by a command SUB_CMD_EMV, - use of a key stored in OB_AUTH_KEY_EMV by a cryptographic algorithm SUB_CRYPTALGO_EMV or a command SUB_CMD_EMV. - use of a PIN stored in OB_PIN by a cryptographic algorithm SUB_CRYPTALGO_EMV or a command SUB_CMD_EMV - Use of OB_TRANS by a command SUB_CMD_EMV or a cryptographic algorithm SUB_CRYPTALGO_EMV.
General rules		
<ul style="list-style-type: none"> - 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; 		

**FDP_ACC.2.2/
SEC_EMV** 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.

SFP : TLV_EMV/EMV Application Proprietary TLV Object Access Control SFP

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

Subjects	Objects	Operations among subjects and objects
SUB_CMD_EMV	OB_APTLV	<ul style="list-style-type: none"> - update and read of data element stored in OB_APTLV by SUB_CMD_EMV;
General rules		

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 40/99

- SUB_CMD_EMV 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;
- Refinement : these operations concern data exchange with the current user of the TOE_EMV, not the TOE_EMV internal exchanges.

**FDP_ACC.2.2/
TLV_EMV** 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.

5.1.7 ACCESS CONTROL FUNCTIONS (FDP_ACF)

5.1.7.1 FDP_ACF.1 Security attribute based access control


SFP : CMD_EMV / EMV Command Access Control SFP

**FDP_ACF.1.1/
CMD_EMV** The TSF shall enforce the **EMV Command Access Control SFP** to objects based on the, following attributes.

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

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

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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 41/99

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

SUB_CMDMAN_EMV shall activate no SUB_CMD if **Card Life Cycle Status** indicates Card is 'dead'

SUB_CMDMAN_EMV shall activate no SUB_CMD except GET DATA if **Card Life Cycle Status** indicates Card is Disabled or Blocked

SFP : FILE_EMV / EMV File Access Control SFP

**FDP_ACF.1.1/
FILE_EMV** The TSF shall enforce the **EMV File Access Control SFP** to objects based on the following attributes

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

Attributes name	Rules
Command File Type,	1. Any SUB_CMD_EMV 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_EMV 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 3. Any SUB_CMD_EMV shall have access to OB_DFILE or OB_EFILE only if the File Header LRC is not corrupted;
File Access Conditions	
File Type	
Card Security Status group	
File Header LRC	


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

- 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_EMV** The TSF shall explicitly deny access of subjects to objects based on the following additional rules : **none**

SFP : SEC_EMV / EMV Secret Access Control SFP

**FDP_ACF.1.1/
SEC_EMV** The TSF shall enforce the **EMV Secret Access Control SFP** to objects based on the, following security attributes.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 42/99

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.

Attributes name	Rules
Key Type	1. Any SUB_CRYPTALGO_EMV shall use a key only if the Key Type security attribute matches the Cryptographic Algorithm Type ;
Cryptographic Algorithm Type	2. Any SUB_CRYPTALGO_EMV shall use a key only if the Ratification group does not indicate the key is blocked. This applies to personalization phases 4 to 6;
Ratification group	
Key Checksum	3. Any SUB_CMD_EMV shall use a PIN only if the Ratification group does not indicate the PIN is blocked;
PIN Checksum	4. No SUB_CRYPTALGO_EMV shall use OB_AUTH_KEY_EMV if Key Checksum indicates data is corrupted ;
Card security Status group	5. No SUB_CRYPTALGO_EMV shall use OB_PIN if PIN checksum indicates data is corrupted;
Command key security attribute	6. A SUB_CRYPT_ALGO_EMV shall use OB_TRANS only if Card Security Status Group indicates Administrator has been correctly identified and Application Block Flag is not set.
Random seed checksum	7. A SUB_CMD_EMV shall use OB_TRANS if allowed by Command Key security attribute .
Application Block Flag	8. No SUB_CRYPTALGO_EMV shall use OB_AUTH_KEY_EMV if Random seed checksum indicates data is corrupted

**FDP_ACF.1.3/
SEC_EMV**

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

**FDP_ACF.1.4/
SEC_EMV**

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:


1. No SUB_CMD_EMV shall have update access to OB_AUTH_KEY_EMV;
2. No SUB_CMD_EMV shall have update access to OB_PIN during phases 4 to 6;
3. No SUB_CMD_EMV shall have read access to OB_AUTH_KEY_EMV and OB_PIN;

SFP: TLV_EMV/ EMV Application Proprietary TLV
**FDP_ACF.1.1/
TLV_EMV**

The TSF shall enforce the **EMV Application Proprietary TLV Object Access Control SFP** to objects based on the **following security attributes**.

**FDP_ACF.1.2/
TLV_EMV**

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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 43/99

Attributes name	Rules
Card Life Cycle Status	1. Any SUB_CMD_EMV 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_EMV 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_EMV shall have access to OB_APTLV only if the TLV Life cycle security attribute is consistent with the Card Life Cycle Status security attribute;
TLV Life cycle	
TLV Read Access List	
TLV Update Access List	
TLV Object LRC	

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

FDP_ACF.1.4/
TLV_EMV
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;**
3. **TLV Object LRC is corrupted;**

5.1.8 DATA AUTHENTICATION (FDP_DAU)

5.1.8.1 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_EMV** with the ability to verify evidence of the validity of the indicated information.

5.1.9 EXPORT TO OUTSIDE TSF CONTROL (FDP_ETC)

5.1.9.1 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1
The TSF shall enforce the **EMV File Access Control and EMV 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.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 44/99

5.1.10 IMPORT FROM OUTSIDE TSF CONTROL (FDP_ITC)

5.1.10.1 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **EMV File Access Control and EMV 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**.

5.1.11 RESIDUAL INFORMATION PROTECTION(FDP_RIP)

5.1.11.1 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 **de-allocation of the resource** to the following objects : **OB_RAM**

5.1.12 STORED DATA INTEGRITY (FDP_SDI)


5.1.12.1 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. **TLV Object LRC**
3. **Key Checksum**

Refinement : LRC integrity error applies only to Application Proprietary TLV Object stored under a OB_EFILE file for Card Risk management.This include OB_TRANS object.PIN checksum

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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 45/99

5.1.13 AUTHENTICATION FAILURES (FIA_AFL)

5.1.13.1 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;**

5.1.14 USER ATTRIBUTE DEFINITION (FIA_ATD)

5.1.14.1 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}**.

5.1.15 USER AUTHENTICATION (FIA_UAU)

5.1.15.1 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.

5.1.15.2 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.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 46/99

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

5.1.15.3 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.**

5.1.16 USER IDENTIFICATION (FIA_UID)

5.1.16.1 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.

5.1.17 USER-SUBJECT BINDING (FIA_USB)

5.1.17.1 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.

5.1.18 MANAGEMENT OF FUNCTION IN THE TSF (FMT_MOF)

5.1.18.1 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 following phases :**

- 1. Administrator Authentication SF_AUTH (phases 4 to 6);**
- 2. Secure Secret Data Loading SF_SDL (phases 4 to 6);**
- 3. Transaction certification SF_TRANS (phase 7).**

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 47/99

5.1.19 MANAGEMENT OF SECURITY ATTRIBUTES (FMT_MSA)

5.1.19.1 FMT_MSA.1 Management of security attributes

**FMT_MSA.1.1/
FILE_EMV** The TSF shall enforce the **EMV Command Access Control and EMV File Access Control SFPs** to restrict the ability to **perform the following operations on the following** security attribute **to the Administrator role and to phases 4 to 6.**

Security attribute	Operation	Phase(s)
File type	create	4 to 6
Card Life Cycle Status	modify	4 to 6

**FMT_MSA.1.1/
SEC_EMV** The TSF shall enforce the **EMV Command Access Control and EMV 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
Application Block Flag	Set and Reset	7

5.1.19.2 FMT_MSA.2 Secure security attributes

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

5.1.19.3 FMT_MSA.3 Static attribute initialization


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

**FMT_MSA.3.2/
CMD_EMV** 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_EMV** The TSF shall enforce the **EMV 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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 48/99

session;

2. **The Command File Type security attribute is set during ES development and cannot be changed.**
3. **The security attributes File Type, File header LRC, must be provided by the Administrator when the object is created.**
4. **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_EMV**

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_EMV**

The TSF shall enforce the **EMV 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 the PIN and Key Ratification group are provided by the Administrator when the object is created;

The Keys and PIN checksum are derived from these objects creation;

The security attribute Random Seed Checksum is set by construction;

Application Block Flag default value is set by construction;

**FMT_MSA.3.2/
SEC_EMV**

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_EMV**

The TSF shall enforce the **EMV 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.

TLV object LRC is provided by administrator when TLV object is created.

**FMT_MSA.3.2/
TLV_EMV**

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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 49/99

5.1.20 MANAGEMENT OF TSF DATA (FMT_MTD)

5.1.20.1 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:**

- Create cryptographic key (phases 4 to 6) : OB_KEY_EMV;
- Create Random Seed : OB_RND_SEED

5.1.21 SECURITY MANAGEMENT ROLES (FMT_SMR)

5.1.21.1 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.

5.1.22 CLASS FMT : ACTIONS TO BE TAKEN FOR MANAGEMENT

Function	Actions
FCO_NRO.1	Managing changes to information types field, originator attributes and recipients of evidence.
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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 50/99

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
FTP_ITC.1	Configuring the actions that requires trusted channel ,if supported

5.1.23 UNOBSERVABILITY (FPR_UNO)

5.1.23.1 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**.

Refinement : Here, 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_EMV	create/update PIN	OB_PIN
SUB_CMD_EMV	create key	OB_KEY_EMV, OB_AUTH_KEY_EMV
SUB_CMD_EMV	comparison of PIN value with reference	OB_PIN
SUB_CRYPTALGO_EMV	use	OB_KEY_EMV, OB_AUTH_KEY_EMV


5.1.24 FAIL SECURE (FPT_FLS)

5.1.24.1 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. **Application proprietary TLV object integrity failure;**
4. **EEPROM programming failure**

Refinement : Preservation of secure state concerns here only events occurring during

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 51/99

standard TSF operation and does not include failures due to physical attacks which are described in FPT_PHP.3

5.1.25 TSF PHYSICAL PROTECTION (FPT_PHP)

5.1.25.1 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
Low clock frequency	Reduction of clock frequency to stop the TOE during a specific operation
High clock frequency	Increase clock frequency to corrupt TOE operation behaviour
Low temperature/high temperature	Attempts to corrupt TOE operations
Low Voltage/High voltage	Set supply voltage out of range

5.1.26 DOMAIN SEPARATION (FPT_SEP)

5.1.26.1 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.


5.1.27 INTER-TSF BASIC DATA CONSISTENCY (FPT_TDC)

5.1.27.1 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**

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 52/99

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;

5.1.28 TSF SELF TEST (FPT_TST)

5.1.28.1 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.

5.1.29 INTER-TSF TRUSTED CHANNEL (FTP_ITC)

5.1.29.1 FTP_ITC.1 Inter-TSF trusted channel

- FTP_ITC.1.1** The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
- FTP_ITC.1.2** The TSF shall permit the **remote trusted IT product** to initiate communication via the trusted channel
- FTP_ITC.1.3** The TSF shall initiate communication via the trusted channel for **TSF Data configuration operation.**

Refinement: This applies to TSF Data configuration functions during phase 4 to 6.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 53/99

5.2 TOE security functional requirements for B0' application


5.2.1 DEFINITION OF B0' SUBJECT, OBJECTS AND ATTRIBUTES

5.2.1.1 Subjects

Subjects/objects name	Description
SUB_CMDMAN_B0'	Process that receives and interpret the command messages sent by the remote IT product
SUB_CMD_B0'	Process activated on SUB_CMDMAN_B0' request according to a specific command message. SUB_CMD_B0' is an object for SUB_CMDMAN_B0'. As SUB_CMD_B0' performs operations on objects listed below, SUB_CMD_B0' is therefore an subject for these objects.

5.2.1.2 Objects


Objects	Type	Description
OB_SECRET	User data /TSF data	EEPROM B0' Secret area that contains following objects : OB_KEY_B0', OB_KEY_CO, OB_KEY_CB, OB_CC1, OB_CC2, OB_KEY_FAB.
OB_KEY_B0'	TSF data	Secret Keys set used for transaction certification.
OB_KEY_CO	User data	Administrator Keys CO (opening key).
OB_KEY_CB	User data	Administrator Keys CB (Bank key).
OB_KEY_FAB	User data	Administrator Keys in personalization phase (Fabrication key).
OB_CC1	User data	User PIN code 1 that may be changed and replaced in usage phase by OB_CC2
OB_CC2	User data	User PIN code 2
OB_TRANSITORY_STATUS	TSF data	EEPROM B0' status area used in personalization phase. This area contains card security information related to Administrator authentication failures.
OB_STATUS	TSF data	EEPROM B0' status area used in usage phase. This area contains card security information related to Administrator or User authentication failures.
OB_CONFIDENTIAL	User data	EEPROM B0' confidential area containing transaction data in usage phase.
OB_TRANSACTION	User data	EEPROM B0' transaction area containing transaction data in usage phase.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 54/99


Objects	Type	Description
OB_FREE	User data	EEPROM B0' free read access area . This area contains public information like mask number, serial number, that can be read by the application . It contains the OB_FAB that is used by the ES.
OB_FAB	User data	EEPROM memory area that defines EEPROM memory partition and access conditions (with pointers addresses and validity information) and life cycle phases.
OB_RAM	TSF data	Entity in RAM containing cryptographic variables used for cryptographic computation and data used for command processing.
OB_CERT	User data	Data encrypted by the TOE for transaction certification

5.2.1.3 Security Attributes

Security Attributes names	Description
Command_Format_B0'	B0' protocol command format (operation codes :CLA, INS)
Command_Parameters	Parameters : A1-A2 Addresses length, D1-D2 Data length, L number of bytes to exchange.
Memory Pointer values	Contains EEPROM memory partition addresses. Pointers values must be consistent. Pointers must be valid
Life Cycle locks [LU,LC,LF,IV,IV]	Life cycle locks are used to switch TOE_B0' from one phase to another. When changing phase corresponding locks is set to 0. [LU,LC,LF,IV,IV] = [1,1,0,1,1] personalization phase [LU,LC,LF,IV, IV] = [1,0,0,1,1] User phase with OB_CC1 [LU,LC,LF,IV,IV] = [0,0,0,1,1] User phase with OB_CC2 [LU,LC,LF,IV,IV] = [x,x,x,0,1] or [x,x,x,1,0] or [x,x,x,0,0] invalidation.
Parameters [E/L]	Defines OB_TRANSACTION Read/Write protection E : Write access ; 1=free; 0= protected L : Read access; 1=free; 0= protected
Parameters[ECa, ECb , EF,EA]	Defines OB_TRANSACTION erase protection EA = Automatic erasure option ; [0] set ; [1] not set ; EF = 1 Not erasable; 0 Erasable but protected by key presentation Eca, Ecb : key to use [1,1] = no key ; [1,0] = OB_CC1 or OB_CC2 ; [0,1] = OB_CO; [0,0] = OB_CB

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 55/99

Security Attributes names	Description
Parameters [E1,L1,EC1a,EC1b,EF1]	OB_CONFIDENTIAL Read/Write/erase protection E1 : Write access ; 1=free; 0= protected L1 : Read access; 1=free; 0= protected EF1 = 1 Not erasable; 0 Erasable but protected by key presentation Ec1a, Ec1b : key to use [1,1] = no key ; [1,0] = OB_CC1 or OB_CC2 ; [0,1] = OB_CO; [0,0] = OB_CB
Parameters[EFM]	OB_STATUS erase conditions : indicates if OB_STATUS may be erased automatically by TSF when it reaches saturation state. EFM=1 not erasable; 0 erasable. This security attribute is internally used by the TSF to manage TSF data OB_STATUS and does not appear in FDP_ACF.1
System bit (V,C,CA) :	System bits used for write/read protection of each word : V is the write validation bit , C and CA indicates the authority authorized to write the word according to following rules: [0,x] = OB_KEY_FAB or OB_CC1 or OB_CC2; [1,0] = OB_CO; [1,1] = OB_CB
Status_Win	OB_STATUS active window that records and indicates authentication failures during usage phase (7) with the following values: 1ERR_CCx: 1 OB_CCx presentation error 2ERR_CCx : 2 successive OB_CCx presentation error ERR_CO/CB : blocked by OB_CO or OB_CB presentation error ERR_BK : blocked by 3 successive OB_CCx presentation error This area limited in size indicates it's own 'Saturation state' as soon as 1 bit in the last word of the area is written. Note : CCx stands for CC1 or CC2
Transitory_Status_Win	OB_TRANSITORY_STATUS active window that records and indicates authentication failures during personalization phase with the following values:[Blocked]
Presentation Status [Octet_Pres, Resultat]	The Presentation Status indicates if a Key/code has been previously presented (Octet_Pres) and if the result of Key/code presentation was valid or no(Resultat)
Keys Checksum	Checksum attached to each key or key area, and used to check their integrity
CCx Checksum	Checksum attached to each CCx and used to check their integrity
Pointers Checksum	Checksum attached to pointers area and used to check their integrity

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 56/99

5.2.2 SECURITY AUDIT ANALYSIS (FAU_SAA)

5.2.2.1 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. **Life Cycle Locks discrepancy**
2. **EEPROM programming failures**
3. **Authentication data integrity failure;**
4. **Pointers address discrepancy;**
5. **Pointers area integrity failure**

b) Other rule: **none**.

5.2.3 CRYPTOGRAPHIC KEY MANAGEMENT (FCS_CKM)

5.2.3.1 FCS_CKM.3 *Cryptographic key access*

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

5.2.3.2 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, **Making Key Unavailable** that meets the following standard : **none**.

Refinement : when changing life cycle from one phase to another, there is no possible access to the previous phase Key.

5.2.4 CRYPTOGRAPHIC OPERATIONS (FCS_COP)

5.2.4.1 FCS_COP.1 *Cryptographic operations*

FCS_COP.1.1 The TSF shall perform **TSF Data certification** in accordance with a specified cryptographic algorithm, **Triple DES** and cryptographic key size of **16 bytes** that meet the following standards: **ANSI X3.92 and B4-B0' V3 (Only in phase 7)**.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 57/99

5.2.5 ACCESS CONTROL POLICY (FDP_ACC)

5.2.5.1 FDP_ACC.2 Complete access control

SFP : CMD_B0'/ B0' Command Access control

FDP_ACC.2.1/ The TSF shall enforce the **B0' Command Access Control SFP** on the **subject**
CMD_B0' **SUB_CMDMAN_B0'** and **all the objects SUB_CMD_B0'**, and all operations among
subjects and objects covered by the SFP.


Subjects	Objects	Operations among subjects and objects
SUB_CMDMAN_B0'	SUB_CMD_B0'	<ul style="list-style-type: none"> - activation of SUB_CMD_B0' by SUB_CMDMAN_B0' - execution of SUB_CMD_B0'
General rules		
<ul style="list-style-type: none"> - Only SUB_CMDMAN_B0' can activate a SUB_CMD_B0' upon receipt of a command message; - SUB_CMD_B0' shall be activated only if the command message corresponds to a supported internal process and is valid ; - SUB_CMD_B0' shall be executed only if command parameters are valid and execution authorized in the current life cycle state. 		

FDP_ACC.2.2/ The TSF shall ensure that all operations between any subject in the TSC and any object
CMD_B0' within the TSC are covered by an access control SFP.

SFP : MEM_B0'/ B0' Memory Access control

FDP_ACC.2.1/ The TSF shall enforce the **SFP B0' Memory Access control** on **all the subjects**
MEM_B0' **SUB_CMD_B0'** that allow direct access to objects **OB_CONFIDENTIAL,**
OB_TRANSACTION, OB_FREE, OB_FAB, and all operations among subjects and
objects covered by the SFP.

Subjects	Objects	Operations among subjects and objects
SUB_CMD_B0'	OB_CONFIDENTIAL OB_TRANSACTION OB_FREE OB_FAB	<ul style="list-style-type: none"> - Read, Read valid, - Write, Write valid, Erase,
General rules		

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 58/99

<ul style="list-style-type: none"> - SUB_CMD_B0' shall have access to data element(s) stored in, OB_CONFIDENTIAL and OB_TRANSACTION according to these areas own protection in read/write/erase access; - OB_FREE shall be read free access after personalization phase; - OB_FAB is written during personalization phase by correctly authenticated administrator. In User phase (7) only read access to this object from the outside shall be allowed; <p><u>Refinement</u> : All operations concern exchange with TOE_B0' user , not internal TOE_B0' exchange.</p>

Note : OB_SECRET objects do not appear in B0' memory Access Control SFP ,but are described in B0' Secret Access Control SFP.


**FDP_ACC.2.2/
MEM_B0'** 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.

SFP : SEC-B0' / B0' Secret Access control

**FDP_ACC.2.1/
SEC_B0'** The TSF shall enforce the **B0' Secret Access Control SFP** on **all the subjects SUB_CMD_B0'** and **all the objects OB_KEY_FAB, , OB_KEY_CO, OB_KEY_CB, OB_CC1, OB_CC2, OB_CERT**, and all operations among subjects and objects covered by the SFP.

Subjects	Objects	Operations among subjects and objects
SUB_CMD_B0'	OB_KEY_FAB OB_KEY_CO OB_KEY_CB OB_CC1 OB_CC2 OB_CERT	<ul style="list-style-type: none"> - Write, write valid, - Certification, - Present key ,
General rules		
<ul style="list-style-type: none"> - Key Presentation must always be followed by a validation (read/write) - OB_KEY_FAB is loaded by the IC manufacturer during phase 3 and no access to this object from the outside shall be allowed afterwards. - OB_KEY_CO, OB_KEY_CB, OB_CC1 are loaded during personalization phase. In User phase (7) no access to this object from the outside shall be allowed after personalization; - OB_CC2 shall only be updated using OB_CC1. <p><u>Refinement</u>: All operations concern exchange with TOE_B0' user , not internal TOE_B0' exchange.</p>		

FDP_ACC.2.2/ 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.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 59/99

SEC_B0'

5.2.6 ACCESS CONTROL FUNCTIONS (FDP_ACF)

5.2.6.1 FDP_ACF.1 Security attribute based access control

SFP : CMD_B0'/ B0' Command Access control

FDP_ACF.1.1/
CMD_B0' The TSF shall enforce the **B0' Command Access Control SFP** to objects based on the following attributes.


FDP_ACF.1.2/
CMD_B0' The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed :

Attributes name	Rules
Command_Format_B0'	1. No SUB_CMD_B0' shall be activated if command_format_B0' is not correct.
Memory Pointers values	2. No SUB_CMD_B0' shall be activated if active pointer value is not consistent with Memory pointers values or in case of Life Cycle Locks discrepancy .
Pointers Checksum	3. No SUB_CMD_B0' shall be activated if one Memory Pointer value is not valid and Life Cycle locks indicate usage phase or Pointers checksum indicate integrity failure
Life Cycle locks [LU,LC,LF,IV,IV]	4. SUB_CMD_B0' Write, Write valid, Erase shall not execute if Life Cycle locks indicate invalidation or if Status_Win or Transitory_Status_Win indicate saturation
Status_Win	5. SUB_CMD_B0' Read valid shall not execute if Status_Win or Transitory_Status_Win indicates saturation and Life Cycle Locks do not indicate invalidation.
Transitory_Status_Win	6. SUB_CMD_B0' Certification shall not execute if Life Cycle locks indicate invalidation. SUB_CMD_B0' Certification shall not execute if one Memory pointer value is not valid and Life Cycle Locks indicate personalization phase.

FDP_ACF.1.3/
CMD_B0' The TSF shall explicitly authorize access of subjects to objects based on the following additional rules : **none**.

FDP_ACF.1.4/
CMD_B0' The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- Any SUB_CMD_B0' shall not execute if **Command_Parameters are not consistent** with expected relevant SUB_CMD_B0' parameters.
- SUB_CMD_B0' Read, and Certification are not allowed if **Command_Parameters A1-A2** does not belong to a readable area .
- SUB_CMD_B0' Write, Write valid and erase are not allowed if **Command_Parameters A1-A2** does not belong to a writable area according to **Life**

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 60/99


Cycle Locks Phase.

SFP : MEM_B0'/ B0' Memory Access control

FDP_ACF.1.1/ MEM_B0' The TSF shall enforce the **B0' Memory Access Control SFP** to objects based on the following attributes.

FDP_ACF.1.2/ MEM_B0' The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed :

Attributes name	Rules
Life Cycle locks [LU,LC,LF,IV,IV]	1. No SUB_CMD_B0' is allowed on OB_CONFIDENTIAL or OB_TRANSACTION if respectively access is protected with Parameter[E1] or [E] and one of the following case occurs :
Parameter[E/L] Parameters[ECa,ECb, EF] Parameters : [E1, L1, EC1a,EC1b,EF1]	<ul style="list-style-type: none"> - Presentation_Status result is not consistent with expected result ,according to System Bit (V,C, CA), - Status_Win indicates ERR_CCx and System Bit (C) is set to 1, - Status_Win indicates Blocked and Presentation_Status indicates that no key has been presented
Presentation Status [Octet_Pres, Resultat]	
System Bit (V,C,CA)	2. SUB_CMD_B0' Write is not allowed on any object if access is protected by Parameter[E1] or [E] or System Bit (V) indicates word is already validated. 3. SUB_CMD_B0' Write valid is not allowed on any object if Status_Win indicates ERR_CCx or ERR_CO/CB and System Bit (V) indicates word is already validated. SUB_CMD_B0' Write valid is not allowed on object if System Bit (V) indicates word is already validated and Life Cycle Locks LF is set.
Status_Win	
Attributes name	Rules
Status_Win	4. SUB_CMD_B0' Read valid is not allowed if Status_Win indicates blocked and Presentation Status indicates no key has been presented.
Presentation Status [Octet_Pres, Resultat]	5. SUB_CMD_B0' Read valid is not allowed on object if Status_Win indicates ERR_CCx and Presentation Status result indicates key presentation was OB_KEY_CO or OB_KEY_CB.
Parameter[E/L] Parameters[ECa,ECb, EF]	6. SUB_CMD_B0' Read and Read validation are not allowed on OB_CONFIDENTIAL or OB_TRANSACTION if respectively access is protected with parameter [L1] or [L] and Presentation Status result is not correct.
Parameters : [E1, L1, EC1a,EC1b,EF1]	7. SUB_CMD_B0' Erase is not allowed on OB_CONFIDENTIAL or OB_TRANSACTION if access is protected with respectively Parameters [EF1] or Parameters [EF] .

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 61/99

Attributes name	Rules
	8. SUB_CMD_B0' Erase is not allowed on OB_CONFIDENTIAL or OB_TRANSACTION if access is protected with respectively Parameters [EC1a, EC1b] or Parameters [ECa, ECb] and Presentation_Status result is not correct .

**FDP_ACF.1.3/
MEM_B0'** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules :

When **Life Cycle locks** indicate personalization phase;

- SUB_CMD_B0' Write valid and Erase are allowed on OB_CONFIDENTIAL and OB_TRANSACTION if **Presentation_Status** indicates OB_KEY_FAB has been presented
- SUB_CMD_B0' Write valid is allowed on OB_FAB if **Presentation_Status** indicates OB_KEY_FAB has been presented


**FDP_ACF.1.4
MEM_B0'** The TSF shall explicitly deny access of subjects to objects based on the following additional rules : **none**

SFP : SEC-B0' / B0' Secret Access control

**FDP_ACF.1.1/
SEC_B0'** The TSF shall enforce the **B0' Secret Access Control SFP** to objects based on the following attributes

**FDP_ACF.1.2/
SEC_B0'** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed

Attributes name	Rules
Keys Checksum	1. No SUB_CMD_B0' is allowed on OB_KEY_CO, OB_KEY_CB or OB_CCx if Keys Checksum , respectively CCx Checksum indicates integrity failure.
CCx Checksum	2. SUB_CMD_B0' Present Key is not allowed on OB_KEY_CB or OB_KEY_CO if Life Cycle locks indicates personalization phase or Status_Win indicates card blocked
Life Cycle locks [LU,LC,LF,IV,IV]	3. SUB_CMD_B0' Present Key is not allowed on OB_KEY_FAB or OB_CCx if Life Cycle locks indicates personalization phase and Command Parameter L is different from 4 or if Status_Win indicate card is blocked.
Status_Win	4. SUB_CMD_B0' Present Key with Unblock Key (CB + CCx) is not allowed if Life Cycle locks indicates personalization phase or Status_Win indicate card is not blocked.
Command Parameter	5. SUB_CMD_B0' Present Key is not allowed on any key or code if Command Parameter length is not coherent with key or code length.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 62/99

Parameter[E/L] Parameters : [E1, L1, EC1a, EC1b, EF1]	6. SUB_CMD_B0' Certification is not allowed on an OB_CERT, and Command Parameter A1-A2 indicates word to certify is not in a readable area or Parameter [L] or [L1] indicates a read protected area.
--	--

**FDP_ACF.1.3/
SEC_B0'**

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules :

- SUB_CMD_B0' Write and Write valid are allowed on OB_CC2 if **Life Cycle Locks LC** is set and if **Presentation_Status** indicates OB_CC1 code has been correctly presented.
- SUB_CMD_B0' Write valid and Erase are allowed on OB_KEY_CO, OB_KEY_CB and OB_CC1 if **Life Cycle Locks** indicates personalization phase and **Presentation_Status** indicates OB_KEY_FAB has been correctly presented.

**FDP_ACF.1.4/
SEC_B0'**

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

5.2.7 DATA AUTHENTICATION (FDP_DAU)

5.2.7.1 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, **OB_KEY_CO, OB_KEY_CB, OB_CCx,**

FDP_DAU.1.2

The TSF shall provide **Specific SUB_CMD_B0'** with the ability to verify evidence of the validity of the indicated information.

Refinement : Specific SUB_CMD_B0' means that only SUB_CMB_B0' which need to use these objects have the ability to verify this evidence.

5.2.8 EXPORT TO OUTSIDE TSF CONTROL (FDP_ETC)


5.2.8.1 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1

The TSF shall enforce the **B0'Memory Access Control SFP** 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.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 63/99

5.2.9 IMPORT FROM OUTSIDE TSF CONTROL (FDP_ITC)

5.2.9.1 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the **B0'Memory Access Control SFP** and **B0' Secret Access Control** 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**.

5.2.10 RESIDUAL INFORMATION PROTECTION(FDP_RIP)

5.2.10.1 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 **de-allocation of resource** to the following object : **OB_RAM**.

5.2.11 STORED DATA INTEGRITY (FDP_SDI)

5.2.11.1 FDP_SDI.2 Stored data integrity monitoring and action

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


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

5.2.12 AUTHENTICATION FAILURES (FIA_AFL)

5.2.12.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **the following numbers** of unsuccessful authentication attempts occur related to the **following authentication events**.

1. **One unsuccessful authentication following a successful authentication as Administrator during phase 4 to 6;**
2. **Three successive unsuccessful authentications as Administrator during phase 4 to 6;**
3. **One unsuccessful authentication as Administrator during phase 7;**

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 64/99

4. **Three successive unsuccessful authentication End-User 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 (from phase 4 to 6) : definitely deny the use of the TOE_B0' ;**
2. **Administrator Authentication and End-User authentication (phase 7) : block the TOE_B0' (mute) until the TOE_B0' is unblocked by authorized Administrator and authorized End-User;**

5.2.13 USER ATTRIBUTE DEFINITION (FIA_ATD)

5.2.13.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users :
Status_Win ; Presentation Status [Octet_Pres, Resultat]

5.2.14 USER AUTHENTICATION (FIA_UAU)

5.2.14.1 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1

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

- **Read validation**
- **Write validation**

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.

5.2.14.2 FIA_UAU.3 Unforgeable authentication

FIA_UAU.3.1

The TSF shall **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.

5.2.14.3 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1

The TSF shall prevent reuse of authentication data related to :

- **Card Personalizer authentication in phase 6.**

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 65/99

5.2.15 USER IDENTIFICATION (FIA_UID)

5.2.15.1 FIA_UID.1 Timing of identification

FIA_UID.1.1

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

- **Read validation**
- **Write validation**

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.

5.2.16 USER-SUBJECT BINDING (FIA_USB)

5.2.16.1 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.

5.2.17 MANAGEMENT OF FUNCTION IN THE TSF (FMT_MOF)

5.2.17.1 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 security functions** to the **following** roles,

- **Administrator with End-User on SF_STATUS (unblocking)**
- **End-User on SF_KEY_CODE (changing Code to CC2)**


5.2.18 MANAGEMENT OF SECURITY ATTRIBUTES (FMT_MSA)

5.2.18.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1/

MEM_B0'

The TSF shall enforce the **B0' Memory Access Control SFPs** to restrict the ability to **perform the following operations on the following** security attribute **to the Administrator role and to phases 4 to 6.**

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 66/99

Security attribute	Operation	Phase(s)
Memory Pointers values	Create	4 to 6
Parameters[E/L]	Create	4 to 6
Parameters [ECa, Ecb,EF,EA]	Create	4 to 6
Parameters [E1, L1,EC1a, EC1b,EF1]	Create	4 to 6
Parameter [EFM]	Create	4 to 6
System bits (V,C,CA)	Create	4 to 6

**FMT_MSA.1.1/
SEC_B0'**

The TSF shall enforce the **B0' Secret Access Control SFPs** to restrict the ability to **perform the following operations on the following security attribute to the Administrator role and to phases 4 to 6.**

Security attribute	Operation	Phase(s)
Parameters[E/L]	Create	4 to 6
Parameters [E1, L1,EC1a, EC1b,EF1]	Create	4 to 6

Refinement : Life cycle change Status can be changed only in following order : from LF to LC , from LC to LU.

At any time User is allowed to set one or both IV invalidation bits , whatever other Locks values are set.

5.2.18.2 FMT_MSA.2 Secure security attributes


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

5.2.18.3 FMT_MSA.3 Static attribute initialization

**FMT_MSA.3.1/
CMD_B0'** The TSF shall enforce the **B0' Command Access Control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

**FMT_MSA.3.2/
CMD_B0'** The TSF shall allow **no role** to specify alternative initial values to override the default values when an object or information is created.

- **The Command Format and command parameters are set during ES development and cannot be changed.**
- **The Locks values are set to default value '1' by construction,**
- **Memory pointers values are provided by the Administrator during usage phase and pointers area Checksum is calculated by TSF when Lock is changed to LC.**
- **Status_Win and Transitory_Status_Win are set by construction and then managed**

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 67/99

by the TSF.

**FMT_MSA.3.1/
MEM_B0'**

The TSF shall enforce the **B0' Memory 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 by the ES for static attributes. By construction the EEPROM is in an erased state and all bits value is 1.

- The Locks values are set to default value '1' by construction,
- Parameters [E,L], [ECa,ECb,EF,Ea],[E1,L1,EC1a,EC1b,EF1], [EFM] and System Bits (V,C,CA) must be provided by the Administrator during personalization phase,
- Status Win default value is set by construction and cannot be changed,
- Presentation Status [Octet Pres,Resultat] is reset to [no, KO] by ES after read validation and write validation operations.

**FMT_MSA.3.2/
MEM_B0'**

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_B0'**

The TSF shall enforce the **B0' 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 by the ES for static attributes. By construction the EEPROM is in an erased state and all bits value is 1.

- Command parameters are set during ES development and cannot be changed.
- The Locks values are set to default value '1' by construction,
- Parameters [E,L], [E1,L1,EC1a,EC1b,EF1] must be provided by the Administrator during personalization phase,
- Presentation Status [Octet Pres,Resultat] is reset to [no, KO] by ES after read validation and write validation operations,
- Key and codes checksum are derived from Keys and codes creation.

**FMT_MSA.3.2/
SEC_B0'**

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


5.2.19 MANAGEMENT OF TSF DATA (FMT_MTD)

5.2.19.1 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 **following roles and to the indicated phases:**

Roles	actions
-------	---------

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 68/99

Administrator	<ul style="list-style-type: none"> - Create OB_KEY_B0' during personalization (phase 4 to 6). - Modify OB_TRANSITORY_STATUS and OB_STATUS (phase 4 to 6).
----------------------	---

5.2.20 SECURITY MANAGEMENT ROLES (FMT_SMR)

5.2.20.1 FMT_SMR.1 Security roles

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

1. **Administrator:** This role has the capability to create the memory partition , configure this memory access condition and load secret data in the TOE_B0' by the knowledge of the Fabrication key during personalization phase 4 to 6.

During phase 7 , the Administrator has the capability to unblock the TOE_B0' with his OB_KEY_CB, (together with the End-User using his OB_CCx code) ,


2. **End-User:** 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; The End-User may change his code from OB_CC1 to OB_CC2;

The End-User has the capability to unblock the TOE_B0' using his OB_CCx code (together with the Administrator using his OB_CB key)

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

5.2.21 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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 69/99

FMT_MTD.1	Managing the group of roles that can interact with the TSF data
-----------	---

There are no other management activities foreseen for the B0' Application embedded in the TOE.

5.2.22 UNOBSERVABILITY (FPR_UNO)

5.2.22.1 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**.

Refinement : Here, unobservability means impossibility to obtain the value of an information during an operation on this information.

Subject	Operation	Object
SUB_CMD_B0'	Compare with reference value	OB_CCx
SUB_CMD_B0'	Compare with reference value	OB_KEY_CO, OB_KEY_CB, OB_KEY_FAB
SUB_CMD_B0'	Use	OB_KEY_B0'

5.2.23 FAIL SECURE (FPT_FLS)

5.2.23.1 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 event**
2. **EEPROM programming failures**


Refinement : Preservation of secure state concerns here only events occurring during standard TSF operation and does not include failures due to physical attacks which are described in FPT_PHP.3

5.2.24 TSF PHYSICAL PROTECTION (FPT_PHP)

5.2.24.1 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
---------	-----------------------------

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 70/99

Low clock frequency	Reduction of clock frequency to stop the TOE during a specific operation
High clock frequency	Increase clock frequency to corrupt TOE operation behaviour
Low temperature/high temperature	Attempts to corrupt TOE operations
Low Voltage/High voltage	Set supply voltage out of range

5.2.25 DOMAIN SEPARATION (FPT_SEP)

5.2.25.1 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.

5.2.26 INTER-TSF BASIC DATA CONSISTENCY (FPT_TDC)

5.2.26.1 FPT_TDC.1 Inter-TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **Administrator Keys(code) and End-user code 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 : **Refer to B4 B0' V3 specification (see 12.2)**

5.2.27 TSF SELF TEST (FPT_TST)


5.2.27.1 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 :

- **At start-up,**
- **After receiving a command message,**
- **each time the lock value is changed or checked**

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.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 71/99

6 TOE SECURITY ASSURANCE REQUIREMENTS

The Assurance requirements is EAL 4 augmented by components :

- ADV_IMP.2 : Implementation of the TSF,
- ALC_DVS.2 : sufficiency of security measures,
- AVA_VLA.4 : Highly resistant.

6.1.1 CONFIGURATION MANAGEMENT (ACM)

EAL4 claimed level requires the following ACM class components:

- ACM_AUT.1 Partial CM automation
- ACM_CAP.4 Generation support and acceptance procedures
- ACM_SCP.2 Problem tracking CM coverage

Refer to CC Part 3 for description.

6.1.2 DELIVERY AND OPERATION (ADO)

EAL4 claimed level requires the following ADO class components:

- ADO_DEL.2 Detection of modification
- ADO_IGS.1 Installation, generation, and start-up procedures

Refer to CC Part 3 for description.

6.1.3 DEVELOPMENT (ADV)

EAL4 augmented claimed level requires the following ADV class components:


- ADV_FSP.2 Fully defined external interfaces
- ADV_HLD.2 Security enforcing high level design
- ADV_IMP.2 Implementation of the TSF
- ADV_LLD.1 Descriptive low-level design
- ADV_RCR.1 Informal correspondence demonstration
- ADV_SPM.1 Informal TOE security policy model

Refer to CC Part 3 for description.

6.1.4 GUIDANCE DOCUMENT (AGD)

EAL4 claimed level requires the following AGD class components:

- AGD_ADM.1 Administrator guidance

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 72/99

AGD_USR.1 User guidance

Refer to CC Part 3 for description.

6.1.5 LIFE CYCLE SUPPORT (ALC)

EAL4 claimed level requires the following ALC class components:

ALC_DVS.2 Sufficiency of security measures

ALC_LCD.1 Developer defined life-cycle model

ALC_TAT.1 Compliance with implementation standards

Refer to CC Part 3 for description.

6.1.6 TESTS (ATE)

EAL4 augmented claimed level requires the following ATE class components:

ATE_COV.2 Analysis of coverage

ATE_DPT.1 Testing high level design

ATE_FUN.1 Functional testing

ATE_IND.2 Independent testing- sample

Refer to CC Part 3 for description.

6.1.7 VULNERABILITY ASSESSMENT (AVA)


EAL4 augmented claimed level requires the following AVA class components:

AVA_MSU.2 Misuse analysis

AVA_SOF.1 Strength of TOE security function evaluation

AVA_VLA.4 Highly resistant

Refer to CC Part 3 for description.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 73/99

7 TOE SUMMARY SPECIFICATIONS

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

7.1 Statement of TOE security function

This part covers the IT security functions and specifies how these functions satisfy the TOE security functional requirement with :

- the security function supplied by the Integrated Circuit and used by the ES,
- the security functions supplied by startup management and used by both application EMV and B0',
- the security functions specific to each application EMV and B0'.

7.1.1 SECURITY FUNCTION SUPPLIED BY THE IC

The security functions listed here after are described in the IC Security Target referenced in section 12.2

7.1.1.1 *F_RND Random Number Generator*

This function produces random numbers with a length of one byte. Each byte will at least contain a 7 bit entropy.

7.1.1.2 *F_DEA Triple DES coprocessor*

This function provides a Triple Des Data Encryption Algorithm (TDEA) of the Data Encryption Standard (DES) as defined by FIPS PUB 46 and supports the 2-key Triple DEA algorithm according to keying option 2 in FIPS PUB 46-3.


7.1.1.3 *F_OPC Control of operation condition*

This function will detect that the TOE is operating outside authorized limits and will reset the chip when one of the following events occurs:

- Low frequency of clock input or,
- High frequency of clock input or,
- Low voltage power supply or,
- High voltage power supply or,
- Low temperature or,
- High temperature .

7.1.1.4 *F_PHY Protection against physical manipulation*

This function protects the TOE against manipulation of the hardware, the software stored in ROM or EEPROM and the data contained in EEPROM and RAM.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 74/99

7.1.1.5 *Permutational or Probabilistic Security mechanisms*

Strength of functions implemented by the IC, is claimed by the IC security target compliant with PP/9806 (see reference in section 12.2). The claimed strength in the IC Security Target is SOF_High and therefore is aligned with the PP/9911 Platform Security Target claimed strength.

7.1.2 SECURITY FUNCTION FOR THE PLATFORM

This section describes the security function used for the platform startup and security function shared by both B0' and EMV applications.

7.1.2.1 *SF_START : Start-up Management*

This function manages RESET and start-up operations.

7.1.2.2 *SF_TST_CODE : Rom code testing*

This function allows authorized user to verify the integrity of the executable TSF stored code. This include both EMV and B0' applications.

7.1.3 STATEMENT OF TOE SECURITY FOR EMV APPLICATION

7.1.3.1 *SF_ACC : Data Access Control*

This SF manages the access to the data elements by the command subjects SUB_CMD_EMV. 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.

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;
- Backup File descriptor during file creation ;

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.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 75/99

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.

7.1.3.2 SF_AUTH : Administrator Authentication

This function ensures the management of the :

- Mutual Authentication during phase 4 to 6 , that is Administrator Authentication and TOE self authentication,
- Administrator Authentication during usage phase (phase 7).

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

7.1.3.3 SF_BKP : Backup Management

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


7.1.3.4 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;

7.1.3.5 SF_CMP : Secure Comparison

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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 76/99

7.1.3.6 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;
- Card Authentication cryptogram computation : CBC-MAC using a double length session key;
- Application Cryptogram computation : CBC-MAC using a double length key;
- ROM code hashing, using DES and Triple DES.

7.1.3.7 SF_DRV : Chip Driver

This function ensures the management of the chip security features :

- EMV start state analysis,
- Record audit events,
- Perform shield actions according to violation severity;

The following auditable events are accounted during a session :

1. Card Life Cycle Status discrepancy;
2. EEPROM programming error;
3. File structure integrity failure;
4. Application proprietary TLV object integrity;
5. Authentication data integrity failure;
6. Configuration integrity failure;
7. Random seed integrity error


Note : During a session the hardware events that might occur (Low voltage, high voltage, low frequency, high frequency, high temperature, Low temperature) are detected and managed by the IC.(see description in 7.1.1)

Any of these hardware events will reset the TOE.

7.1.3.8 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);

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 77/99

- Key value and header, containing the key attributes (maximum presentation number, ratification, size, key type, key LRC);
- Application Proprietary TLV Object including Transaction Specific Data used to generate Application cryptogram.

In case of integrity failure, the event will be notified to SF_DRV.

7.1.3.9 SF_KEY : Cryptographic Key Management

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

- Key search;
- Key verification;
- Key read;
- Key transfer;
- Key destruction;
- Key ratification management;

7.1.3.10 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 2, 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.

7.1.3.11 SF_PIN : PIN Management


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

- PIN search;
- PIN verification;
- End-User Authentication;
- PIN modification;

This function uses only authentic values (value that has been presented) to perform its operations

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

Note : the SF_PIN security function uses SF_RAT Security function to achieve the SOF-High of the authentication mechanism.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 78/99

7.1.3.12 SF_RANDOM : Software random management

This function generates the TOE Software Random Number :

This function calculates and checks the Random Seed integrity each time it is used. In case of integrity failure, the use of authentication or cryptographic keys will be denied, and the function will notify the event to SF_DRV.

7.1.3.13 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;

7.1.3.14 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_EMV, 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.

7.1.3.15 SF_SDL : 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 ensures Secure Messaging which is used for secure transmission of command messages.

- Integrity : a Message Authentication Code is added to the command message to guarantee the integrity of the message and to authenticate the source of the message.
- Confidentiality : the data field of the message is enciphered before transmission to guarantee the confidentiality of the transmitted data.


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

7.1.3.16 SF_TRANS : Transaction Application Cryptogram generation

According to the received Terminal Command parameters, this function will allow to generate the Application Cryptogram related to the current transaction.

This function will :

- check if the application is not blocked ,
- check if the Administrator has been correctly authenticated, using SF_AUTH,
- check the integrity of the concerned data using SF_INT,

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 79/99

- generate the authenticated Administrator associated Application Cryptogram using SF_CRY,
- return the response message containing Application cryptogram and execution status.

Note : This security function ensures Issuer commands reception (script) during online transaction before 2nd Generate AC..

7.1.3.17 SF_TST : Self Test

This function allows to Check the TOE_EMV configuration checksum and card life cycle :

- during startup,
- after receiving a command message.

In case of failure, the event will be notified to SF_DRV.

7.1.3.18 Permutational or Probabilistic Security mechanisms

The following table shows which security mechanisms are used in the implementation of each claimed SOF_High function.

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

Table 3 : Mapping of the security mechanisms and the IT security functions for EMV application


7.1.4 STATEMENT OF TOE SECURITY FOR B0' APPLICATION

7.1.4.1 SF_CERTIFICATION : Data certification

This function is used to generate User Data certification ensuring that this data has not been corrupted.

The function will :

- interpret the certification command parameters (random number, data to be certified address, key set to use),
- access secret key set with a specific access method ,

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 80/99

- use triple DES encryption on the data to be certified to generate the required certificate

If the secret key set is not found, card will be turned in mute state.

7.1.4.2 SF_CHECK : Check pointers

This function will check:

- Memory pointers addresses values coherence,
- Memory pointers validity,

If memory pointers are not coherent or not valid in usage phase card will be turned mute.

7.1.4.3 SF_COMMAND_B0':Command analyzer

This function will analyze command parameters coherence according to command to be processed , for data length, and addresses .

In case of error the command process will be aborted and TOE turned mute.

This function also checks if command parameter A1-A2 belongs to a readable area when executing Read or Certification operations, or to a writable area when executing Write, Write valid or Erase operation.

7.1.4.4 SF_DES_B0':DES computation

This function ensures the cryptographic computation of triple DES for B0' application.

This function is supported by the IC security function F_DEA.

7.1.4.5 SF_DISPATCH : Command dispatching

This function ensures the initialization of B0' application after execution of SF_START.

7.1.4.6 SF_DRV_B0':EEPROM programming failure

This function ensures the detection of EEPROM programming failures .


7.1.4.7 SF_BKP_B0': Backup mechanism

This function ensures that TSF preserves a secure state in case of unexpected abortion of it's execution during the updating of the TSF security status area (OB_STATUS,OB_TRANSITORY_STATUS).

7.1.4.8 SF_INT_B0': Integrity Check

This function will perform the following operations:

- Calculate the checksum of keys codes and memory pointers area,
- Check the integrity of Keys, codes and memory pointers area before they are used,

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 81/99

If an error occurs, the TOE will perform the following action:

- Clear RAM ,
- Turn the TOE mute.

7.1.4.9 SF_KEY_CODE : Key/code presentation

When a key or code is presented, this function will:

- Check the card current phase and the card security status (card blocked/ error), using SF_LOCK_B0' and SF_STATUS.
- check Key/code length ,
- check Key/code integrity using SF_INT_B0',
- Compare Key/code value with the values stored in the TSF using SF_SECRET.

If the key/code presented is not consistent with the card security status, or in case of integrity failure, the TOE will be turned mute.

Strength of this function is SOF-High.

7.1.4.10 SF_LOCK_B0' : Life Cycle locks management

This function allows to manage life cycle locks:

- Read current locks value ,
- Change the TOE life cycle stage by writing the locks value to the next allowed phase in a determined order for the life cycle locks LF,LC,LU, and at any time for the IV locks,
- Check for locks discrepancy each time locks are changed and turn the TOE mute in case of discrepancy.

When a lock is set, there is no possibility to go back to the previous stage. When one of the IV lock is set, the TOE is permanently invalidated.

At the end of the manufacturing phase the lock LF is set by the IC manufacturer putting TOE in personalization phase, and allowing the use of the Card manufacturer authentication key. (IC_FAB).

At the end of personalization , the LC lock is set, putting the TOE in Usage phase , disabling the use of the card manufacturer authentication key. (IC_FAB) and enabling the use of Code CC1.

When LU is set this disable code CC1 usage and enable code CC2 usage.


When a lock is changed, this function will use SF_INT_B0' to calculate user and TSF data integrity.

7.1.4.11 SF_MEM_ACCESS : Memory access

This function controls the memory access rights according to read/write/erase protection attributes.

This function will be used to check before any of these operation execution :

- The protection of the area addressed by the operation according to security attributes Parameters[E,L] , Parameters [E1,L1,EC1a,EC1b,EF1]Parameters[ECa, Ecb, EF,EA], System bit (V,C,CA)
- When an access to an area is protected, checks if Key/code presentation was successful.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 82/99

If access is not granted, TOE will be turned mute.

7.1.4.12 SF_SECRET: Secure use of secret

This function will ensure :

- The secure secret Keys access using a Random Reading Method,
- The secure secret Keys loading,
- The secure use and comparison of Authentication Keys and Codes,
- The de-allocation of memory after secret key manipulation and after each command execution.

7.1.4.13 SF_STATUS : Security Status management

According to life cycle status, this function will record the following events :

- Each read validation operation on a read access protected area,
- Any write validation operation on a write protected area if :
 - The key/code previously presented is wrong,
 - The previous status indicates a fail state or blocked state and the key/code presented is correct.

According to these recordings, this function will indicate a blocked state after the following events:

- One unsuccessful authentication following a successful authentication as Administrator during phase 4 to 6;
- Three successive unsuccessful authentication as Administrator during phase 4 to 6;
- One unsuccessful authentication as Administrator during phase 7;
- Three successive unsuccessful authentication End-User during phase 7.

This function use SF_BKP_B0' before execution .

7.1.4.14 Permutational or Probabilistic Security mechanisms

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

	SF_CERTIFICATION	SF_CHECK	SF_COMMAND_B0'	SF_DES_B0'	SF_DISPATCH	SF_DRV_B0'	SF_BKP_B0'	SF_INT_B0'	SF_KEY_CODE	SF_LOCK_B0'	SF_MEM_ACCESS	SF_SECRET	SF_STATUS
Administrator authentication									x				
End user authentication									x				


	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 83/99

Table 4 : Mapping of the security mechanisms and the IT security functions for B0' application


7.2 Statement of assurance measures

This chapter defines the list of the assurance measures required for the TOE security assurance requirement compliant with the EAL4 augmented . Augmentation includes ADV_IMP.1,2 ; ALC_DVS.1,2; AVA_VLA.2,4

The assurance measures are fully described in the referenced documents.

These measures concern only the ES development (both application EMV and B0') as required by PP/9911. Measures concerning the IC development and manufacturing are described in the IC Security Target referenced in section 12.1.

Assurance requirement	Assurance measure
ASE Security Target evaluation	[document reference]
ACM_AUT.1 Partial CM automation	[document reference]
ACM_CAP.4 Generation support and acceptance procedures	[document reference]
ACM_SCP.2 Problem tracking CM coverage	[document reference]
ADO_DEL.2 Detection of modification	[document reference]
ADO_IGS.1 Installation, generation and start-up procedures	[document reference]
ADV_FSP.2 Fully defined external interfaces	[document reference]
ADV_HLD.2 Security enforcing high level design	[document reference]
ADV_IMP.2 Implementation of the TSF	[document reference]
ADV_LLD.1 Descriptive low-level design	[document reference]
ADV_RCR.1 Informal correspondence demonstration	[document reference]
ADV_SPM.1 Informal TOE security policy model	[document reference]
AGD_ADM.1 Administrator guidance	[document reference]
AGD_USR.1 User guidance	[document reference]
ALC_DVS.2 Sufficiency of security measures	[document reference]
ALC_LCD.1 Developer defined life cycle model	[document reference]
ALC_TAT.1 Compliance with implementation standards	[document reference]
ATE_COV.2 Analysis of coverage	[document reference]
ATE_DPT.1 Testing High-level design	[document reference]
ATE_FUN.1 Functional testing	[document reference]
ATE_IND.2 Independent testing- sample	[document reference]
AVA_MSU.3 Analysis and testing for insecure state	[document reference]

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 84/99

Assurance requirement	Assurance measure
AVA_SOF.1 Strength of TOE security function evaluation	[document reference]
AVA_VLA.4 Highly resistant	[document reference]

Table 5 : Statement of assurance measures

8 PP CLAIMS


8.1 PP reference

The PP “Smart Card Integrated Circuit with Embedded software Protection Profile” V2.0 registered at the French Certification Body under the number PP/9911 is claimed.

8.2 PP refinement


The following functional requirements found in the claimed PP are refined both form EMV and B0' applications.

Component	Iteration	Assignment	Selection	Refinement
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				

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 85/99

Component	Iteration	Assignment	Selection	Refinement
FPT_TDC.1		x		
FPT_TST.1		x	x	

Table 6 : Mapping of the performed operations and the IT security functional requirements

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 86/99

The following functional requirements found in the claimed PP are refined for EMV application.

Component	Iteration	Assignment	Selection	Refinement
FCO_NRO.1		x	x	
FTP_ITC.1		x	x	

8.3 PP additions

8.3.1 ASSETS REFINEMENT

Application Data have been refined from PP/9911 assets definitions :

- Secret data like secret keys and Pin codes
- Transaction Specific Data used by the TOE to perform its security function during an CB-EMV transaction.

8.3.2 ADDITIONAL ASSUMPTIONS

There are no additional assumptions to PP/9911 but the following PP assumptions have been refined :

A.USE_PROD (phase 4 to 6)

A.USE_DIAG (phase 7)

8.3.3 ADDITIONAL ORGANIZATION SECURITY POLICY

Organizational Security Policy are application dependant and have not been defined in the PP/9911.


This ST defines the following Organizational Security Policies as required by the need for compliance with EMV and B0' applications.

OSP.CB_EMV	TOE is designed to be conform to CB-EMV specifications
OSP.B0'	TOE is designed to be conform to B0' specifications
OSP.CRYPTO	TOE shall respect the French laws on the cryptographic usage
<i>OSP.REPUD_EMV</i>	<i>TOE contributes to the non-repudiation of a transaction processed by the TOE on behalf of the authorized card holder for CB-EMV application .</i>
OSP.TOE_AUTH_EMV	TOE provides means to be authenticated by the IT remote system during phase 4 to 6 of CB-EMV application card manufacturing process.
OSP.TOE_LOGO	A mark allowing to identify the IC manufacturer is visible on the IC.

8.3.4 ADDITIONAL THREATS

The following threats has been added to PP/9911 threats , for CB-EMV application specific requirements

<i>T.MOD_TR_EMV</i>	<i>Unauthorized modification of Transaction Specific Data stored and used by the TOE during its function processing and during usage phase (phase 7)for CB-EMV application</i>
---------------------	--

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 87/99

8.3.5 ADDITIONAL SECURITY OBJECTIVES

The following security objectives have been refined from PP/9911:

O.TEST_OPERATE (phase 4 to 6)

O.USE_DIAG (phase 7)

The following security objective has been added to PP/9911 objectives.

O.REPUD_EMV (phase 7)

O.TOE_AUTH_EMV (phase 4 to 6)

O.DEV_DIS_ES_SPEC (phase 1)

O.TOE_LOGO (IC manufacturing: phase 3)

8.3.6 ADDITIONAL SECURITY FUNCTIONAL REQUIREMENTS

Security functional requirements have been added to the claimed PP to meet CB-EMV specific security requirements.

FCO_NRO.1 : Selective proof of origin

FTP_ITC.1 : Inter-TSF trusted channel

8.3.7 ADDITIONAL ASSURANCE REQUIREMENTS FROM PP/9911

There are no additional assurance requirements from the PP statements in this ST.

9 RATIONALE

This section presents evidence to be used for the ST evaluation. This evidence supports the claims that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.


9.1 Security objectives rationale

All PP/9911 Assumptions, Threats and Security Objectives are included in this ST. Therefore, the rationale contained in the PP/9911 is sufficient for the ST and is not repeated here. Only PP refinement or PP additional elements are discussed below.

Additional elements have no impact on the PP9911 threats and objectives consistency, neither on the PP9911 rationale.

This section demonstrates that :

- Security objectives refinements satisfy PP/9911 Assumptions refinement,
- At least one security objective is correlated to the additional threat,
- Additional security objectives satisfy the Organizational Security Policy.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 88/99

9.1.1 ASSUMPTIONS ADDRESSED BY OBJECTIVES

A.USE_DIAG has been refined to take in account specific application security rules that are supposed to be followed by the administrator and user in usage phase (phase 7).

O.USE_DIAG objective which is defined in PP/9911 to satisfy the A.USE_DIAG assumption, has been also refined in this ST to satisfy the A.USE_DIAG refinement.

The assurance requirement EAL4 contributes to the satisfaction of the refined O.USE_DIAG, as AGD class will ensure that these recommendations are added to Administrator and User guidance that are generated.

9.1.2 THREATS AND SECURITY OBJECTIVES

T.MOD_TR_EMV addresses CB-EMV application Transaction Specific Data, used by the TOE to perform its security functions. These data are loaded during phase 4 to 6 during personalization process, and used during phase 7. They have to be protected in integrity before use

O.MOD_MEMORY addresses TOE sensitive information stored in memories that have to be protected against any corruption or unauthorized modification and therefore addresses also T.MOD_TR_EMV

9.1.3 ORGANIZATIONAL SECURITY POLICY ADDRESSED BY OBJECTIVES

O.DEV_DIS_ES_SPEC addresses the Organizational security policies OSP.EMV, OSP.B0' and OSP.CRYPTO.

This objective is satisfied by the EAL4 ADV class requirement that will ensure that the product is developed according to the required specification.

O.REPUD_EMV addresses the Organizational Security Policy OSP.REPUD_EMV for the TOE in its CB-EMV application transaction operations during phase 7.

O.TOE_AUTH_EMV addresses the Organizational Security Policy OSP.TOE_AUTH_EMV for the TOE in the CB-EMV card manufacturing process during phases 4 to 6.

O.TOE_LOGO addresses the OSP.TOE_LOGO.

This objective is satisfied by the EAL4 ADO class. ADO document will provide recommendation to the IC manufacturer as to fulfill this objective.

9.2 Security requirements rationale


This section demonstrates that the set of security requirements (TOE and environment) is suitable to meet the security objectives.

9.2.1 SECURITY FUNCTIONAL REQUIREMENT RATIONALE

The ST contains all PP/9911 objectives and security functional requirements. PP/9911 is not repeated here. Only additional objectives and additional security functional requirements are discussed below.

Additional elements have no impact on the PP9911 objectives and Functional requirement consistency, neither on the PP9911 rationale, except that additional objectives are also satisfied by existing functional requirements as shown in the table below.

This section demonstrates that the combination of additional objectives for the TOE are suitable to satisfy additional security functional requirements.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 89/99

The table below shows which functional requirement contributes to the satisfaction of additional objectives.

Objectives/ Functional requirements	O.REPUD_EMV	O.TOE_AUTH_EMV
FCO_NRO.1	X	
FTP_ITC.1		X
FCS_CKM.3	X	
FCS_COP.1	X	
FIA_UAU.3.		X
FIA_UAU.4		X

FCO_NRO.1 Non repudiation of origin satisfies O.REPUD_EMV, ensuring that the TSF generate evidence of origin for the information Transaction Specific Data.

FCS_CKM.3 : Cryptographic key access and FCS_COP.1 : Cryptographic operations, ensure the generation of this evidence of origin through cryptographic means and contribute also to satisfy O.REPUD_EMV.

FTP_ITC.1 Inter-TSF Trusted channel satisfies O.TOE_AUTH_EMV, ensuring that the TOE will provide a secure communication channel between itself and the remote trusted IT.

FIA_UAU.3 : Unforgeable Authentication and FIA_UAU.4 : Single-use authentication mechanism, contribute also to the non repudiation of the transaction and therefore satisfy also O.TOE_AUTH_EMV.

9.2.2 SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCIES

In this ST, only additional functional requirements to PP/9911 are discussed.

FCO_NRO.1 is hierarchical to no other component, and has dependencies on FIA_UID.1 which is included in PP/9911 functional requirement and therefore in this ST.

FTP_ITC.1 is hierarchical to no other component and has no dependencies.


The additional functional requirements used in this ST are compatible and coherent with PP/9911 functional requirement

9.2.3 SECURITY ASSURANCE REQUIREMENTS

The list of assurance requirements defined in chapter “ assurance measures ” are those of the claimed Protection Profile EAL4 augmented, and are sufficient for the ST.

9.3 TOE summary specification rationale

The rationale is Gemplus property

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 90/99

9.4 PP claims rationale

This security target presents all the PP/9911 threats, assumptions, objectives, assurance measures and functional requirement.

The additional organizational policies are due to the type of application implemented by the ES and these policies are covered by a specific additional objective in the ST.

The PP/9911 assumptions refinement are covered by existing PP/991 objectives refinement.

Threat T.MOD_TR_EMV (modification of transaction data) has been added to clarify CB-EMV requirement to protect Transaction Specific Data from modification. This threat is covered by the objective O.MOD_MEMORY in phase 7.

Organizational Security Policies OSP.CB_EMV, OSP.B0', OSP.CRYPTO and OSP.TOE_LOGO have been added to meet specific requirements for the CB_B0'/EMV product specification. These policies are covered by additional objectives in this ST, and those objectives are covered by the EAL4 assurance measures.

Organizational Security Policy OSP.REPUD_EMV (repudiation of transaction) has been added to meet CB-EMV requirement for the non-repudiation of transaction and is covered by O.REPUD_EMV objective.

Organizational Security Policy OSP.TOE_AUTH_EMV has been added to meet CB-EMV requirement that the TOE shall authenticate itself towards another IT, and is covered by O.TOE_AUTH_EMV objective.

Functional requirement added to the PP/9911 in this ST, are FCO_NRO.1 that addresses O.REPUD_EMV, and FTP_ITC.1 that addresses O.TOE_AUTH_EMV.

FCO_NRO.1 is hierarchical to no other component and has a dependency with FIA_UID.1 which is part of the PP/9911 and this ST.

FTP_ITC.1 is hierarchical to no other components and has no dependencies.

There are no additional assurance measures to PP/9911.

The strength of function claimed is high, and the claimed level is EAL4+ as required by the claimed PP/9911. The IC security functions used by the platform also claim high level and the used IC is compliant to PP9806 level EAL4+.

Therefore, as all additional elements are coherent and do not introduce inconsistency with the PP/9911, PP claim is fulfilled.


10GLOSSARY

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.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 91/99

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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 92/99

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.

Key Security Status security attribute

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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 93/99

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.

Service Provider:

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

Session

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

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 94/99

Silicon Manufacturer.

Chip supplier called sometimes founder.

Short File Identifier

The 5 least significant bits of a file identifier.

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 1.3.2 specification.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 95/99

11 ABBREVIATIONS

AC

Application Cryptogram

AS

Application Software

ATC

Application Transaction Counter

BS

Basic Software

CBC

Cipher-Block Chaining

CC

Common Criteria

DES

Data Encryption Standard

EAL

Evaluation Assurance Level

ECB

Electronic Code Book

EEPROM


Electrically Erasable and Programmable Read Only Memory

EF

Elementary File

ES

Embedded Software

 COMPLUS	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 96/99

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

 COMPLUS	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 97/99

ST

Security Target

TLV

Tag Length Value

TOE

Target of Evaluation

TSC


TSF Scope of Control

TSF

TOE Security Functions

TSP

TOE Security Policy

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 98/99


12 REFERENCES

12.1 TOE references

ES description	Reference	Revision
Gemplus Smart Gem CB-B0'/EMV	GEM CB-B0'/EMV	MPH021
Chip description	Reference	Revision
Philips Smart Card IC	PWE6804	D

12.2 External documents references

Reference	Title
CC part 1	Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model CCIMB - 99-031, Version 2.1, August 1999 (conform to ISO 15408)
CC part 2	Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements CCIMB-99-032, Version 2.1, August 1999 (conform to ISO 15408)
CC part 3	Common Criteria for Information Technology security Evaluation Part 3: Security Assurance Requirements CCIMB-99-033, Version 2.1, August 1999 (conform to ISO norm 15408)
CEM	Common Methodology for Information Technology Security Evaluation CEM-99/045, version 1.0, August 1999.
PP/9806	Protection Profile Smart Card Integrated Circuit Version 2.0 , September 1998
PP/9911	Protection Profile Smart Card Integrated Circuit with Embedded Software Version 2.0 , June 1999.

	Gem CB-B0'/EMV Security Target	Version : Public Date of creation March 2002
		Page number : 99/99

CB_B0'/EMV	Cahier des Charges Technique du produit communautaire CB_B0'/EMV V4.0 Mars 2001
EMV_IC	Exigences de sécurité Microcircuit à contact version 0.6 édité le 04/03/99 par Gie-Cartes Bancaires
EMV_APP	Exigences de sécurités Application Carte de paiement et retrait CB-EMV Version 0.9 édité le 04/03/04/00 par Gie-Cartes Bancaires
EMV_SA	Exigences de sécurités Service d'administration de la carte CB-EMV version 0.10 édité le 07/04/00 Gie-Cartes Bancaires
B0'_SEC	Spécifications de sécurité de l'application B4-B0' V3 Référence : DTE/SEC/SPE/1999-001 version 3.0 date 20/06/00
B0'_STF	Spécifications technique et fonctionnelle du masque B4 B0' Référence : DTE/SEC/SPE/1999-002 version 3.0 date 20/06/00
FIPS PUB 46-3	Federal Information Processing Standards Publication Data Encryption Standard (DES) reaffirmed 1999 October 5.
ST PWE6804	Security Target : Evaluation of the Philips P8WE6804V0 Secure 8-bit Smart Card Controller.

12.3 Internal documents references

Internal references are Gemplus property.

End Of Document.