O.C.S. B0'V3
SECURITY TARGET

State: Reference

Version : V01.00

Contents

1. ST introduction

1.1 ST IDENTIFICATION

Title :

O.C.S. B0'V3 Security Target

Reference:

- Microcontroller ST19SF02*AD RRR of STMicroelectronics*
- ROM : Mask HOST version 6.4
- FUNCTION TYPE (see table below)

FONCTION TYPE	Under evaluation in this security target
B0' V3	Yes
B0' V2	No
B3 : "dual card (HOST and B0')"	No

The main objectives of this evaluation is B0' V3 application : The function B0' in the dual card configuration version will be evaluated through maintenance program processus.

B0'V2 will not be evaluated.

A glossary of terms used in this ST is given in annex A.

This security target refers to the ST19SFxx microcontroller security target [ST19_ST]

1.2 ST OVERVIEW

The intent of this Security Target is to specify functional and assurance requirements applicable to:

- the B0'V3 application.

The main objectives of this Security Target is B0' application:

- to describe the Target of Evaluation (TOE) as a product and position it in the life cycle of the smartcard.
- to describe the security objectives of the TOE and its supporting environment in terms of integrity and confidentiality of application data and programs, protection of the TOE and associated documentation during the development and production phases.
- to describe the security environment of the TOE including the assets to be protected and the threats to be countered by the TOE and by the operational environment during the development production and user phases.
- to specify the security requirements which includes the TOE IT functional requirements, the TOE IT Assurance requirements and the security requirements for the IT environment.

The Assurance level for this ST is **EAL 4 augmented**

1.3 CC CONFORMANCE

The TOE conforms to part 2 and 3 of the common criteria. This is described as follows:

a) **Part 2 conformant** – the security functional requirements are based on those identified in part 2 of the Common Criteria.

b) **Part 3 conformant** – the security assurance requirements are in the form of an EAL or assurance package that is based upon assurance components in part 3 of the Common Criteria.

The CC conformance can be evaluated against the Version 2.1 of the Common Criteria:

- [CC-1] Common Criteria for Information Technology security Evaluation
  Part 1 : Introduction and general model CCIMB-99-031, version 2.1 August 1999,

- [CC-2] Common Criteria for Information Technology security Evaluation

Part 2 : Security Functional Requirements CCIMB-99-032, version 2.1 August 1999,

- [CC-3] Common Criteria for Information Technology security Evaluation

Part 3 : Security Assurance Requirements CCIMB-99-033, version 2.1 August 1999,

When the TOE is mentioned, it comprises the Smart Card IC with B0' application (its Embedded Software) and the scope of the evaluation comprises phases 1 to 3 of the Smart Card life cycle.

The Smart Card IC platform, which is the part of the TOE, is yet certified by the French Certification Body (See certificate 2000/11) under the reference ST19SF02ADxyz and is compliant to the PP/9806 referenced in the French IT Security Evaluation and Certification Scheme. The PP/9806 is dedicated to phases 2 and 3, and to IC design and realization including software manipulation and embedding.

This ST claims the "Smart card Integrated Circuit with embedded Software" Protection Profile (PP) registered and certified under the reference PP/9911 in the French IT Security Evaluation and Certification Scheme. This ST, based on the IC certificate 2000/11 to ensure the PP/9806 conformance, does not include PP/9806 requirements except for coherence with B0' specific functions (See TOE summary).

1.4 OTHER REFERENCE

The TOE conforms to « Spécifications de sécurité de l'application B4-B0'V3 » du groupement CARTES BANCAIRES -[SSAB0']. Some security functional requirements are based on those identified in « ST19SFxx SECURITY TARGET » de STMicroelectronics [ST19_ST].

-[SSAB0'] « Spécifications de sécurité de l'application B4-B0'V3 »
du groupement CARTES BANCAIRES.
ref : DTE/SEC/SPE/1999-001 Version 3.0 du 28/03/00

-[ST19_ST] « ST19SFxx GENERIC SECURITY TARGET » de STMicroelectronics
ref : ST.AZUR.001/0006 version 1_2

2. TOE Description

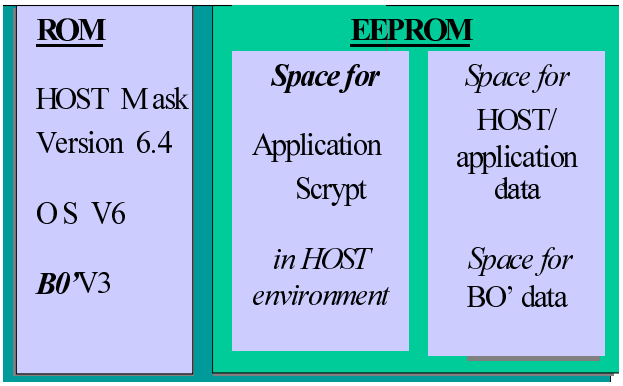
This part of the ST describes the TOE as an aid to the understanding of its security requirements and address the product type, the intended usage and the general features of the TOE.

2.1 PRODUCT TYPE

2.1.1 Introduction

The TOE is made of "Cartes Bancaires" holder based on a smart card. This is a debit card sized card with a non volatile memory (EEprom) and a software embedded within a processor unit. The software is composed of :

- the B0' application configured for a "Cartes Bancaires" holder B4-B0' V3.



The mask is the HOST V6.4 software for the Operating System and the BO' application:

- HOST V6.4 includes OS V6 and B0'V3.

2.1.2 Smartcard

The TOE is a application-based smart card which contains the B0' functionality. The card is a plastic card in ISO format (ISO 7810) and conforms to the ISO Standards 7816/1-2-3.

The B0' card contains an auto-programmable microcomputer with non-volatile EEPROM memory, permitting the storing of secret or confidential data, and with associated circuits that ensure its protection. It answers to the specification B0'V3 Functional Specification of CARTES BANCAIRES and it is implemented in conjunction with the Smart Card operating system HOST Version 6.4 implemented by Oberthur.

The implementation of B0'V3 card follows the various objectives in adherence to the Groupement de Cartes Bancaires, the Transaction Zone of a B0 or B0'V1 or B0'V2 card allows for the storing of transactions.

The EEPROM technology of the components on which the B0'V3 mask is implemented allows for the deletion of the Transaction Zone for a certain number of times. The recycling of this zone prevents premature saturation of the Transaction Zone.The recycling therefore caters for a mandatory economic requirement of high priority.

The B0'V3 functions were implemented without the constraints imposed by the terminals and the applications. B0'V3 must satisfy functional adequacy with the whole of the reference park of banking terminals.

2.1.3 GENERAL PRESENTATION

Groupement des Cartes Bancaires "CB" promotes, develops and ensures the security of the "CB" system, an interbank card system for payment and cash withdrawal. Cartes Bancaires is responsible for coordinating the definition and implementation of general regulations, procedures and specifications relating to "CB" cards and associated technical equipments as well as to the overall operation of the system. It supervises the respect of these rules and promotes the quality and security of the "CB" system.

The smartcard ISSUER is responsible the production of its cards . It is the administrator of access rights to banking services (privative and interbancarity). It transmits to the personnalizater information of necessary configuration for the interbancarity. These parameters fix services CB as well as their limit utilization. It manages secrets of the CB card that it are clean.

It transmits, manages tools of generation, replacement and verification of the confidential code. It organizes and check the distribution to the card holder and necessary information for its utilization. It is the alone ability authority to open or to modify banking services to which it allows to access. Its authority allows it to decide the placement in list of opposition of a card, its gives inoperative and its capture, to recuperate it and to destroy it when its period utilization has expired.

These are banking functions dedicated to the smartcard, but not participating directly to a payment interbanking operation. They are used or not according to the will of the banking institutions and are processed to the holder banking teller by the mean of a dedicated device: the banking device (change of the pin code, change of the holder threshold reading transactions data, recovery of the smartcard, invalidation of the B4-B0' application).

The Telepayment is a remote monetary transaction done by the holder by the mean of the smartcard and a device (telematic, telephonic or televisual) connected to the telepayment server of the Acquirer Bank. This operation contains the same steps as in proximity payment: identifications, flow control and certification (the certificate is checked by the acquirer, delegatee of the issuer.

The smartcard embedded software designer (Oberthur Card Systems) is in charge of the smartcard software development. It is also the software provider. It is responsible of collecting and integrating software and the specification of prepersonnalisation (for Application and OS) requirements.

The IC designer (STMicroelectronics) designs the IC and the IC Dedicated Software. The IC designer provides information, software or tools to the Software designers and Software provider, and receives the software from the software provider , through trusted delivery and verification procedures. It is also the IC manufacturer. It is responsible for producing the IC through three main steps: IC manufacturing, testing, and pre-personnalisation

The smartcard product manufacturer is responsible for the smartcard product finishing process and testing. The application software and data provided by the Software provider are loaded onto the chip at the pre-personnalisation process.

The HOLDER is a person in possession of a CB card. He is the customer of a bank, user of banking functions by his CB card. He is the unique user and holder of secret code associated his card. He can change it with assistance of his bank.

2.1.4 Smartcard Product Life-cycle

The smartcard product life-cycle is decomposed into 7 phases where the following authorities are involved:

Phase 1	Smartcard embedded software development and IC design	The smartcard **embedded software designers** are in charge of the smartcard software development. The **software provider** is responsible of collecting and integrating software and the specification of prepersonnalisation (for Application and OS) requirements. The **IC designer** designs the IC and the IC Dedicated Software. The **IC designer** provides information, software or tools to the Software designers and Software provider, and receives the software from the software provider , **through trusted delivery and verification procedures**.
Phase 2	IC development	From the IC design , Dedicated Software, software, **IC Designer** build the smartcard IC data base, necessary for the IC photomask fabrication.
Phase 3	IC manufacturing and testing	The **IC manufacturer** is responsible for producing the IC through three main steps: IC manufacturing, testing, and pre-personnalisation.
Phase 4	IC packaging and testing	The **IC packaging manufacturer** is responsible for the IC packaging and testing.
Phase 5	Smartcard product finishing process	The **smartcard product manufacturer** is responsible for the smartcard product finishing process and testing. Other application software and data provided by the **Software provider** may be loaded onto the chip at the pre-personnalisation process.
Phase 6	Smartcard personnalisation	The **smartcard issuer** provides the smartcard personnalisation data to the **personnaliser**. The personnaliser is responsible for the smartcard personnalisation and final tests.
Phase 7	Smartcard end-usage	The smartcard issuer is responsible for the smartcard product delivery to the **smartcard end-user**, and the end of life process.

The Figure 1 describes the Smartcard product life-cycle.

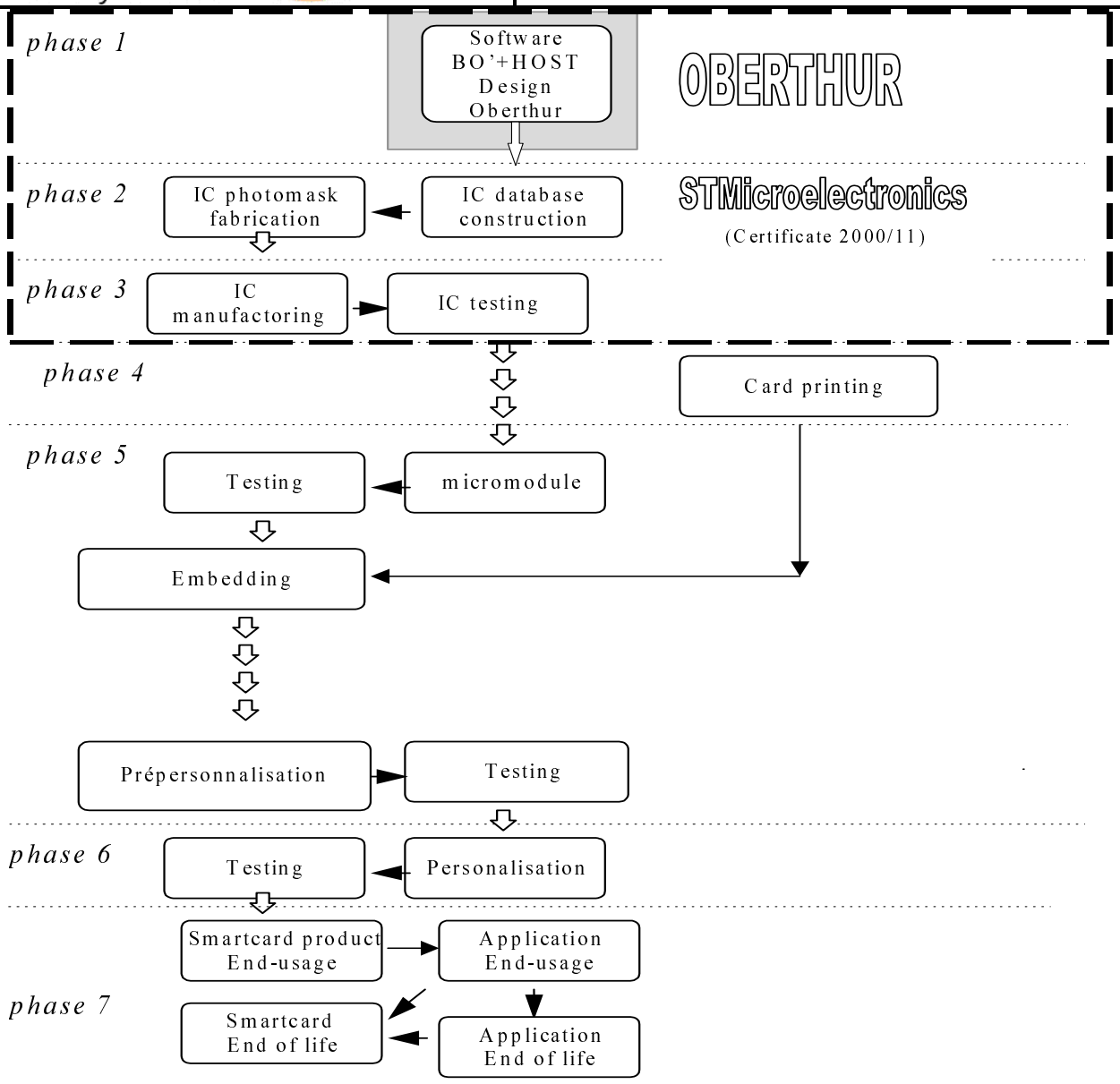


Figure 2 *Smartcard product life-cycle for the B0' application*

The limits of the TOE correspond to the Development and fabrication from phase 1 to phase 3.

These different phases may be performed at different sites; procedures on the delivery process of the TOE must exist and be applied for intermediate delivery of the TOE or the TOE under construction within a phase.

2.1.5 Environment

Considering the composite TOE, three types of environment are defined (see figure 2 and 3):

- Development environment corresponding to phase 1,2.
- Production environment corresponding to phases 3, 4.
- User environment corresponding to phases 5, 6 (start user) and 7 (end user).

2.1.5.1 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 authorised 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 Agreement's.

Design and development of the Operating System then follows. The engineer uses a secure computer system (preventing unauthorised access) to make his specifications, design and development and generation of the TOE. Storage of sensitive documents, databases on tapes, diskettes are in appropriately locked cupboards/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g. shredding).

Integration/validation testing of the TOE components then take place in a secure environment.. During the electronic transfer to IC manufacturer of sensitive programs and data, procedures must be established to ensure that programs and 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).

2.1.5.2 Production environment

During phases of production, the software is stored and transported to be integrated in the IC by the way of the IC manufacturing and the test environment.

Moreover the environment in which these operations takes place must be secured. Storage of sensitive information (photomask, databases on tapes, disks or diskettes) are in appropriate locked cupboard/safe. Of paramount importance also is the disposal of unwanted data (complete electronic erasures) and documents (e.g shredding).

As high volume of Smart Cards are commonly produced, adequate control procedures are necessary to account for all products at all stages.

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

The IC manufacturer environment covers a B0' environment. (It uses a method approved by CB to check and control the integrity and the version of BO' application).

2.1.5.3 User environment

In phase 5, B0' smartcard embedded software is configured into the chip at the packaging process.

In phase 6 (start user TOE) , the personaliser introduces user data including secret keys transmitted by the issuer.

The holder uses his card with the recommendation use given by his bank (approved by CB).

2.2 INTENDED USAGE

The TOE is composed of a BO' banking for credit/debit cards.

During phases 1 to 7, the users of the B0' TOE are the following:

	TOE users (B0' inactive)
Phase 1	- the Software designer **(administrator**) - the Software provider
Phase 2	- the IC designer
Phase 3	- the IC manufacturer
Phase 4	- The printing manufacturer

	TOE users (B0' active : User TOE)
Phase 5	- the smartcard product manufacturer (**administrator**)
Phase 6	- the personnalizer (**administrator**) - the smartcard issuer
Phase 7	- the smartcard issuer (**administrator)** - the smartcard end-user Note: The IC designer, the IC manufacturer, the packaging manufacturer and the smartcard product manufacturer may also receive the TOE stored in ICs for analysis should occur problems during the smartcard usage.

2.3 IT FEATURES

The TOE IT functionalities consist of the following functions :

- **proximity payment:**

  it is a monetary transaction done by the holder at merchant location and in his presence by the mean of a smartcard and the mechant device. This operation is done in three steps:

  - IDENTIFICATIONS:

    the device checks, in user memory, the identification data of the holder and the issuer

  - FLOW CONTROL:

    the device checks, in the smartcard memory, data related with the used banking service and its threshold (maximum amount authorized by the issuer for the cumulative amount of the transactions done on a specific period) in order to determine whether the transaction should lead to call to the issuer authorisation center.

  - CERTIFICATION:

    in case the transaction is processed, the device records, in the smartcard user memory, the date and the transaction amount which are used as inputs, for the B4-B0' application, to issue a transaction certificate which will be checked by the issuer.

- **Telepayment:**

  This is a remote monetary transaction done by the holder by the mean of the smartcard and a device (telematic, telephonic or televisual) connected to the telepayment server of the Acquirer Bank. This operation contains the same steps as in proximity payment: identifications, flow control and certification (the certificate is checked by the acquirer, delegatee of the issuer.

- **"Banking devices" functions:**

  These are banking functions dedicated to the smartcard, but not participating directly to a payment interbanking operation.

  They are used or not according to the will of the banking institutions and are processed to the holder banking teller by the mean of a dedicated device: the banking device.

  Here are, for example, some functions:

  - change of the pin code
  - change of the holder threshold
  - reading transactions data
  - RECOVERY of the smartcard
  - Invalidation of the B4-B0' application

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 organisational security policies and the secure usage assumptions.

3.1 ASSETS

Assets are security relevant elements of the TOE:

The TOE itself (including the code of B0' application) is therefore an asset.

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

The B0' assets that shall be protected are:

- B0' keys
- Holder pin code
- Configuration parameters : Memory configuration parameters, authentication data and B0' Keys.
- B0' user memory data : Status/ Transaction/ Confidential/ Reading/ Fabrication EEPROM area data.

3.1.1 User Data

- B0' keys : These keys are written during the personalisation of the application and are used at use step.
- Status zone data : These data are used to give information on access windows and error windows (on protected zone).
- Transaction zone data : These data are used to give information on the transaction (Date, amount…).
- Confidential zone data : These data are optional.
- Reading zone data : These data are used to give information on Identity data of the B0' application, the cardholder, the Issuer and the Issuer's Delegator. Data are written during the personalisation of the application and are reading at use step.
- Fabrication Zone data : These data are used to give information about Fabrication steps (memory configuration data and security attributes). Data are written during the personalisation of the application and are reading at use step.

- Identity data : data allowing to identify the personaliser, the B0' application, the cardholder, the Issuer and the Issuer's Delegator.

3.1.2 TSF Data

3.1.2.1 Authentication data

- Holder pin code (PIN1 : "Code confidentiel 1" et PIN2 "Code confidentiel 2") : The key PIN1 is written during the personalisation of the application and is used at use step, the key PIN2 is written during the personalisation or use step and both key are used at use step.

- Fabrication Key (Clé de fabrication) : This key is written during the loading of the application and is used at personalisation step.

- Issuer delegated Key (Clé d'ouverture) : This key is written during the personalisation of the application and is used at use step.

- Issuer Key (Clé Banque) : This key is written during the personalisation of the application and is used at use step.

3.1.2.2 Security attributes (or group of security attributes)

- Memory configuration parameters with all pointers allowing to limit the memory zones (Secret/ Status/ Transaction/ Confidential/ Reading/ Fabrication EEPROM area) and access conditions (Read/write/erase) on those memory zones : Those security attributes are written during the personalisation of the application and are used at use step.

3.2 ASSUMPTIONS

The following general assumption is done concerning the TOE:

A.TERM It is assumed that the B0' terminal has capabilities to enter a secure state when a failure occurs during a credit/debit or payment transaction.

3.3 THREATS

3.3.1 BO' DIVULGATION

T_DIVULG_LOGIC Divulgation of the B0' application logical part (B0' code in ROM of the chip)

T_DIVULG_PERSO Divulgation of the identifier of each authority qualified to personalize the chip.

T_DIVULG_USE Divulgation of the identifier of each authority qualified to use or to modify the functions delivered by the chip, that is the one from the issuer, the one from the delegator of the issuer and the one from the holder.

T_DIVULG_CRYPTO Divulgation of the identifier used by the cryptography.

3.3.2 BO' CLONING.

T_CLON_NOT_PERS Substitution of the chip or of the B0' application logical part of a non personalized CB card, that is the consequences of their replacement by a clone on a non personalized CB card.

T_CLON_PERS Substitution of the chip or of the B0' application logical part of a personalized CB card, that is the consequences of their replacement by a clone on a personalized CB card.

3.3.3 BO' USURPATION

T_USPB0_PERS_A Personalisation of the B0' application by entities different from the ones qualified, namely the embedder and the personaliser.

T_USPB0_USE_H Use of proximity payment and telepayment service delivered by the CB system, by the mean of a card, by a user different from the holder.

T_USPB0_PERS_S Personalisation of proximity payment and telepayment service delivered by the CB system, by the mean of a card, by an

entity different from the one qualified, namely the issuer or its delegator.

T_USPB0_USE_C Use of proximity payment and telepayment service delivered by the CB system, by the mean of a card which has not been issued by the qualified issuer.

3.3.4 BO' INTEGRITY CORRUPTED

T_INTEGR_ME8 Non authorised modification of following confidential data:

- the "logical" part of B4-B0' application (chip)
- the identifier of any actor authorized to personalise the programmed IC, that is to say the embedder and the personaliser
- the identifier of any actor authorized to use or to modify the services provided by the programmed IC, that is to say the one of the issuer, the one of the issuer's delegator and the one of the card holder.
- the identifiers used by the cryptography.

T_INTEGR_USE Non authorised modification, in usage phase, of configuration and processing data.

T_INTEGR_ME10 Non authorised modification of any data in invalidation phase.

3.4 ORGANISATIONAL SECURITY POLICIES

An organisational security policy is mandatory for the smartcard B0' product usage.

OSP_CHECK_AV The Authentication Value (A.V.) is an encrypted data written into the user memory of the chip during the personalisation. This A.V. is made of a set of relevant data present into the user memory. The merchant device checks this A.V..

OSP_FLUX_CONT This control is done by the merchant device and allows to limit the amount of monetary transactions done by a single card, without host authorisation during a given period of time.

OSP_BLACK_LIST This is the list of opposed CB cards regularly updated by the acquirer banking institutions and sent to the CB cards acquiring devices.

OSP_SEC_CONV The "CB" Groupement des Cartes Bancaires sets with the embeders and the personalisers a security convention which defines the security demands required to get the security agreement of their company in the concerned domain.

4. 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 during development and delivery process.

4.1 SECURITY OBJECTIVES FOR THE TOE

O. B0_AUTH	The TOE security functions shall ensure authentication of the TOE for all authorized users.
O. B0_TAMPER	The TOE security functions shall prevent physical tampering with its security critical parts.
O. B0_ACCESS	The TOE security functions shall ensure that user data are only accessed by authorized users. It shall prevent unauthorized access to stored memory data.
O. B0_INTEG_DATA	The TOE security functions shall provide the means to avoid unauthorized modification.
O. B0_OPERATE	The TOE security functions shall ensure the continued correct operation of its security functions.
O.B0_FLAW	The TOE must not contain flaws in design, implementation or operation.

4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT

O.B0_ELECTRO_MASKER. It shall ensure that material involved in the electronic microcontroller development are protected.

O.B0_LOGIC_MASKER. It shall ensure that the logical elements in the software development are protected.

O.B0_LOGIC_PRINT. It shall provide the installator a method to check and control the integrity and the version of BO' application.

O.B0_LOGIC_ DELIVER. It shall record flow traceability data to support effective security management.

O.B0_INSTALLATOR. It shall provide a procedure which protects the software elements at installation time.

O.B0_EMBEDDER_DELIVER. It shall provide a procedure which secures the delivery between the IC manufacturer and the embbeder.

O.B0_PERSONALISER_DELIVER. It shall provide a procedure which secures the delivery between the embedder and the personaliser.

O.B0_DEVICE. Methods and DEVICE while in user phase (Phase 7) garantee the integrity and confidentiality of data.

5. TOE security functional requirements for phases 3 to 6

The TOE IT functional requirements define the functional requirements for the TOE using only functional requirements components drawn from the [CC-2].

The minimum strength of function level for the TOE security requirements is SOF-high.

5.1 CLASS FAU SECURITY AUDIT

5.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TOE Security Functions shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

This aspect of the functionality is not applicable: the audit functions are active at any time.

b) not specified.

c) [assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TOE Security Functions shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

Date and time of the event: none in the TOE.

b) No other element.

Iteration	Other specifically defined auditable events
B0'_FAU_GEN	- **Authority Identity (Personaliser) associated to word validation in writing.**

Table 1 : List of defined auditable events for B0'

5.1.2 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 [assignment: *subset of defined auditable event*s] known to indicate a potential security violation;

b) **No other rules**.

Iteration	subset of defined auditable events
B0'_FAU_SAA	- Operating changes by environment, - Access control violation attemps, - Bad EEPROM or CPU usage.

Table 2 : Potential violation analysis

5.2 CLASS FCS CRYPTOGRAPHIC SUPPORT

5.2.1 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].

Iteration	type of cryptographic key access	cryptographic key access method	list of standards
B0'_FCS_CKM01	**Key Management**	**- The personaliser creates (+valid) Cryptographic keys**	**See FS7 and FS8**

Table 3 : Cryptographic key access

5.2.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Iteration	cryptographic key destruction method	list of standards
B0'_FCS_CKM02	**- Physically protection**	**- Key erase mechanism**

Table 4 : Cryptographic key destruction

5.3 CLASS FDP USER DATA PROTECTION

5.3.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TOE Security Functions shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TOE Security Functions shall ensure that all operations between any subject in the TOE Security Functions Scope of Control and any object within the TOE Security Functions Scope of Control are covered by an access control SFP.

Iteration	access control SFP	list of subjects and objects
B0'_FDP_ACC	**access control B0' SFP**	**EEPROM data : Fabrication area and other areas.**

Table 5 : Security attribute based access control for B0'

5.3.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TOE Security Functions shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes*, *named groups of security attributes*].

FDP_ACF.1.2 The TOE Security Functions shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TOE Security Functions shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TOE Security Functions shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Access control SFP	Objects	Security attributes, named groups of security attributes	rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects	rules, based on security attributes, that explicitly authorise access of subjects to objects	rules, based on security attributes, that explicitly deny access of subjects to objects
access control B0' SFP	Fabrication area	Security attributes and rules are in conformity with GIE CB specification -[SSAB0']			

Table 6 : Security attribute based access control for B0'

5.3.3 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TOE Security Functions Scope of Control.

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

Iteration	access control SFP and/or information flow control SFP
B0'_FPD_ETC01	**access control SFP (See FDP_ACF.1)**

Table 7 : Export of user data without security attributes

5.3.4 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

information flow control SFP	list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP
secure sensitive IC test information available in IC TEST configurations (Phase 3)	There is no flow of information from IC test functions in phase 4 to 7 (IC inhibits critical test functionality and supports the non reversibility of the IC configuration)

Table 8 : Subset information flow control

5.3.5 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *the minimum number and type of security attributes*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall provide the following [assignment: *list of additional SFP capabilities*].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

information flow control SFP	the type of security attributes	additional information flow control SFP rules
secure sensitive IC test information available in IC TEST configurations (Phase 3)	**IC configuration is in IC USER CONFIGURATION**	**Configuration of IC shall not be reversible**

Table 9 : Simple security attributes

5.3.6 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [assignment: *access control SFP and/or information flow control SFP*] when importing user data, controlled under the SFP, from outside of the TSC.

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

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rules*].

Iteration	access control SFP and/or information flow control SFP
B0'_FDP_ITC01	**access control SFP (See FDP_ACF.1)**

Table 10 : Import of user data without security attributes

5.3.7 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 [selection: *allocation of the resource to*, *deallocation of the resource from*] the following objects: [assignment: *list of objects*].

.

Iteration	Selection	List of objects
B0'_FDP_RIP	**deallocation of the resource from**	**On one side, the all memory reserved to processing tasks is reinitialized at the beginning of each session. On the other side, the memory containing sensitive data which may jeopardize a function dedicated to the security is also reinitialized between two functions**

Table 11 : Subset residual information protection for B0'

5.3.8 FDP_SDI.2 Stored data integrity monitoring and action

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

FDP_SDI.2.2 **Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*].**

.

Iteration	integrity errors	user data attributes	action to be taken
B0'_FDP_SDI01	**unintentional integrity errors due to Hardware errors**	**user data updating on E²PROM.**	**The Error status « EEPROM Failure » is returned to the terminal after unsuccessfuls tries of writting on EEPROM and the word is not validated on EEPROM.**
B0'_FDP_SDI02	**Loss of integrity affecting E²PROM memories in reading E²PROM data.**	**Data value read from EEPROM.**	**Mute card.**

Table 12 : Stored data integrity monitoring and action for B0'

5.4 CLASS FIA IDENTIFICATION AND AUTHENTICATION

5.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TOE Security Functions shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TOE Security Functions shall [assignment: *list of actions*].

Iteration	Number	List of authentication events	List of actions	Refinement
B0'_FIA_AFL	**3**	**unsuccessful authentication attempts since the last successful authentication**	**disabling of the key authentication**	**Pre-personaliser or Personaliser authentication:** **Unblock is impossible**

Table 13 : Authentication failure handling in phases 5 to 6

5.4.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TOE Security Functions shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

Iteration	List of security attributes
B0'_FIA_ATD	**'Role', 'Access conditions'**

Table 14 : User attribute definition in phases 5 to 6

5.4.3 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

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

Iteration	List of TSF-mediated actions	Refinement
B0'_FIA_UAU01	- Read (Or seek the word) or write without validation of the B0' memory except the two first words - Set up lock bits.	**Before the Personaliser** is authenticated : - The authentication cover the synchronize function.

Table 15 : Timing of authentication for B0'

5.4.4 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.

5.4.5 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment:*identified authentication mechanism(*s)].

Iteration	Identified authentication mechanism(s)
B0'_FIA_UAU02	**Identified authentication mechanism(s) are in conformity with GIE CB specification - [SSAB0']**

Table 16 : Single-use authentication mechanisms iterations

5.4.6 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment: *list of 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 succesfully identified before allowing any other TSF-mediated actions on behalf of that user.

Refinement	List of TSF-mediated actions
Personaliser	- Read (Or seek the word) or write without validation of the B0' memory except the first words include into memory area [200, AD1[, - Set up lock bits.

Table 17 : Timing of identification for B0'

5.4.7 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.

5.5 CLASS FMT : SECURITY MANAGEMENT

5.5.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

Iteration	Selection: determine the behaviour of, disable, enable, modify the behaviour of	list of functions	the authorised identified roles	Refinement
B0'_FMT_MOF01	DISABLE	IC manufacturing phase functions (OS of the IC) And enable Personalisation phase functions (OS of the embedded software)	IC manufacturer	Irreversible function
B0'_FMT_MOF02	DISABLE	Personalisation phase functions	Personaliser Anybody	Irreversible function
B0'_FMT_MOF03	DISABLE	Personalisation phase functions (Invalidation)	Personaliser Anybody	Irreversible function

Table 18 : Management of security functions behaviour in phases 3 to 6

5.5.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TOE Security Functions shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

Iteration	Assignment	Selection	List of security attributes	the authorised identified roles
B0'_FMT_MSA01	access control B0' SFP	create	Access Conditions on EEPROM area : RESERVED, FREE, PROHIBITED	Personaliser

Table 19 : Management of security attributes

5.5.3 FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TOE Security Functions shall ensure that only secure values are accepted for security attributes.

5.5.4 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: *restrictive, permissive, other property*] default values for security attributes that are used to enforce the *SFP*.

FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Iteration	access control SFP, information flow control SFP	Selection	Authorised identified roles
B0'_FMT_MSA 02	**access control B0' SFP**	**- None property : the attribute initialization value is introduced when the attribute is created**	**Nobody**

Table 20 : Static attribute initialisation

5.5.5 FMT_MTD.1 Management of TOE Security Functions data

FMT_MTD.1.1 The TOE Security Functions shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TOE Security Functions data*] to [assignment: *the authorised identified roles*].

Iteration	Selection	list of TOE Security Functions data	Authorised identified roles
B0'_FMT_MTD01	Create (+valid)	- Authentication Keys (CO,CB) - PIN	Personaliser
B0'_ FMT_MTD02	Modify	- Authentication Keys (fab,CO,CB) - PIN	None

Table 21 : Management of TOE Security Functions data

5.5.6 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TOE Security Functions shall maintain the roles [assignment: *the authorised identified roles*].

FMT_SMR.1.2 The TOE Security Functions shall be able to associate users with roles.

Iteration	Authorised identified roles
B0'_FMT_SMR02	Personaliser
B0'_FMT_SMR03	Issuer
B0'_FMT_SMR04	Delegation responsible for Issuer
B0'_FMT_SMR05	Holder

Table 22 : Security roles

5.6 CLASS FPR PRIVACY

5.6.1 FPR_UNO.1 Unobservability*

FPR_UNO.1.1 The TOE Security Functions shall ensure that [assignment: *list of users and/or subjects*] are unable to observe the operation [assignment: *list of operations*] on [assignment: *list of objects*] by [assignment: *list of protected users and/or subjects*].

Iteration	list of users and/or subjects	list of operations	list of objects	list of protected users and/or subjects
B0'_FPR_UNO	external users	- operations of comparison for authentication	user data	TOE

Table 23 : Unobservability

5.7 CLASS FPT PROTECTION OF THE TOE SECURITY FUNCTIONS

5.7.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TOE Security Functions shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*].

Iteration	Refinement	list of types of failures in the TSF
B0'_FPT_FLS01	**Parameters configuration**	**Inconsistent TSF data such as : Key Fab. not initialized and B0' personalization mode.**
B0'_FPT_FLS02	**EEPROM Erasing data**	**Interruption in EEPROM erasing data**

Table 24 : Failure with preservation of secure state for B0'

5.7.2 FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: : *list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

Iteration	physical tampering scenarios	list of TSF devices/elements
B0'_FPT_PHP01	**Analyse the TSF behaviour step by step**	Reduction of clock frequency to stop the TOE during a specific operation.
B0'_FPT_PHP02	**Corrupt TOE operation behaviour**	Increase clock frequency to corrupt TOE operation behavior
B0'_FPT_PHP03	**Corrupt TOE operation behaviour**	Decrease/Increase supply voltage to put the TOE under/over the minimum/maximum operation voltage range
B0'_FPT_PHP04	**Corrupt TOE operation behaviour**	Attempt to access TOE physical layers through access control violations attemps or bad EEPROM /CPU usage.
B0'_FPT_PHP05	**Corrupt TOE operation behaviour**	Attempt to access TOE physical layers.

Table 25 : Resistance to physical attack for B0'

5.7.3 FPT_SEP.1 TOE Security Functions domain separation

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

FPT_SEP.1.2 The TOE Security Functions shall enforce separation between the security domains of subjects in the TOE Security Functions Scope of Control.

5.7.4 FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *list of TSF data types*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

Iteration	list of TSF data types	list of interpretation rules to be applied by the TSF
B0'_FPT_TDC01	**Authentication data value,** **Pointers values consistency**	**GIE CB Specification**

Table 26 : Inter-TSF basic TSF data consistency

5.7.5 FPT_TST.1 TOE Security Functions testing

FPT_TST.1.1 The TOE Security Functions shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TOE Security Functions shall provide authorised users with the capability to verify the integrity of TOE Security Functions data.

This aspect of the functionality is not applicable: the integrity verification of TSF data stored on EEPROM is based on consistency of data, IC technology and EEPROM Stored data integrity monitor (defined in FDP_SDI.2).

FPT_TST.1.3 The TOE Security Functions shall provide authorised users with the capability to verify the integrity of stored TOE Security Functions executable code.

This aspect of the functionality is applicable in case of TSF executable code stored on EEPROM.

Iteration	Selection	Refinement
B0'_FPT_TST	During initial start-up	Application start-up

Table 27 : Security Functions testing

6. TOE security functional requirements for phase 7

The TOE IT functional requirements define the functional requirements for the TOE using only functional requirements components drawn from the [CC-2].

The minimum strength of function level for the TOE security requirements is SOF-high.

6.1 CLASS FAU : SECURITY AUDIT

6.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TOE Security Functions shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

This aspect of the functionality is not applicable: the audit functions are active at any time.

b) not specified.

c) [assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TOE Security Functions shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

Date and time of the event: this has to be interpreted as a sequence of events recognizable by the TOE.

b) No other element.

Iteration	Other specifically defined auditable events
UB0'_FAU_GEN	- **Authority Identity (Issuer, holder, Delegation responsible for issuer) associated to word writing in transactions area or confidential area if reserved writing access.** - **Authentication type (Issuer, Holder) associated to the application blocked status.**

Table 28 : List of defined auditable events for B0'

6.1.2 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 [assignment: *subset of defined auditable event*s] known to indicate a potential security violation;

b) **No other rules**.

Iteration	subset of defined auditable events
UB0'_FAU_SAA	- **Idem for phases 3 to 6**

Table 29 : Potential violation analysis

See description in paragraph for phases 3 to 6

6.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Iteration	Authorised users	List of audit information
UB0'_FAU_SAR01	**Holder, Issuer, Delegation responsible for issuer.**	**- Authority Identity (Issuer, holder, Delegation responsible for issuer) associated to word writing in transactions area or confidential area if reserved writing access.**
UB0'_FAU_SAR02	**Holder, Issuer, Delegation responsible for issuer.**	**- Authentication type (Issuer, Holder) associated to the application blocked status (find in Status area)**

Table 30 : Audit review for B0'

6.2 CLASS FCO COMMUNICATION

6.2.1 FCO_NRO.1 Selective proof of origin

FCO_NRO.1.1 The TSF shall be able to generate evidence of origin for transmitted [assignment: *list of information types*] at the request of the ***recipient***.

FCO_NRO.1.2 The TSF shall be able to relate the [assignment: *list of attributes*] of the originator of the information, and the [assignment: *list of information fields*] 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 [selection: *originator, recipient,* [assignment: *list of third parties*]] given [assignment: *limitations on the evidence of origin*].

Iteration	List of information types	List of attributes	List of information fields	List of third parties	Limitations on the evidence of origin
UB0'_FCO_NRO	**Payment transactions only *under Terminal control***	**CB Card identity (Application Key authentication)**	**Words written in transaction area by the terminal (such as : Payment amount, Payment date, Payment location)**	**GIE CB**	**Infinite**

Table 31 : Enforced proof of origin iterations

6.3 CLASS FCS CRYPTOGRAPHIC SUPPORT

6.3.1 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform [assignment: *type of cryptographic key access*] in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following: [assignment: *list of standards*].

Iteration	type of cryptographic key access	cryptographic key access method	list of standards
UB0'_FCS_CKM01	**Key Management**	**- Nobody can modify Cryptographic keys**	**See FS7 and FS8**

Table 32 : Cryptographic key access

6.3.2 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 [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Iteration	cryptographic key destruction method	list of standards
UB0'_FCS_CKM02	- Physically protection (See FPT_PHP.3)	- Key erase mechanism

Table 33 : Cryptographic key destruction

6.3.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Iteration	List of cryptographic operations	cryptographic algorithm	Cryptographic key sizes	list of standards
UB0'_FCS_COP01	Authentication of B0' application	DES/3DESCryptographic Algorithm and key sizes are in conformity with GIE CB specification -[SSAB0']		Certification scheme B0'V2
UB0'_FCS_COP02	Payment certification			Certification scheme B0'V2
UB0'_FCS_COP03	Authentication of B0' application			Certification scheme B0'V3
UB0'_FCS_COP04	Payment certification			Certification scheme B0'V3

Table 34 : Cryptographic operation for B0'

6.4 CLASS FDP USER DATA PROTECTION

6.4.1 FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TOE Security Functions shall enforce the [assignment: access control SFP] on [assignment: list of subjects and objects] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TOE Security Functions shall ensure that all operations between any subject in the TOE Security Functions Scope of Control and any object within the TOE Security Functions Scope of Control are covered by an access control SFP.

Iteration	access control SFP	list of subjects and objects
UB0'_FDP_ACC	**access control B0' SFP in : Reading (Including the seek of word), Writing, Erasing.**	**EEPROM data : Secret area, Status area, Transactions area, Confidential area, Reading area, Fabrication area.**

Table 35 : Complete access control for B0'

6.4.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TOE Security Functions shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes*, *named groups of security attributes*].

FDP_ACF.1.2 The TOE Security Functions shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TOE Security Functions shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TOE Security Functions shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Access control SFP	**Objects**	**security attributes, named groups of security attributes**	**rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects**	**rules, based on security attributes, that explicitly authorise access of subjects to objects**	**rules, based on security attributes, that explicitly deny access of subjects to objects**
access control B0' SFP	**Secret area**	**Security attributes and rules are in conformity with GIE CB specification -[SSAB0']**			
access control B0' SFP	**Status area**				
access control B0' SFP	**Transactions area**				
access control B0' SFP	**Confidential area**				
access control B0' SFP	**Reading area**				
access control B0' SFP	**Fabrication area**				

Table 36 : Security attribute based access control for B0'

6.4.3 FDP_DAU.1 Basic data authentication

FDP_DAU.1.1 The TOE Security Functions shall provide a capability to generate evidence that can be used as a guarantee of the validity of **Payment Services Data**.

FDP_DAU.1.2 The TOE Security Functions shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information.

Iteration	List of subjects
UB0'_FDP_DAU	**Terminal**

Table 37 : Basic Data authentication iterations

6.4.4 FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TOE Security Functions Scope of Control.

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

Iteration	access control SFP and/or information flow control SFP
UB0'_FPD_ETC01	**access control SFP (See FDP_ACF.1)**

Table 38 : Export of user data without security attributes

6.4.5 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects*, *information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

information flow control SFP	**list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP**
secure sensitive IC test information available in IC TEST configurations (Phase 3)	**Idem phases 3 to 6**

Table 39 : Subset information flow control

See description in paragraph for phases 3 to 6

6.4.6 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *the minimum number and type of security attributes*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall provide the following [assignment: *list of additional SFP capabilities*].

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

information flow control SFP	the type of security attributes	additional information flow control SFP rules
secure sensitive IC test information available in IC TEST configurations (Phase 3)	**Idem phases 3 to 6**	

Table 40 : Simple security attributes

See description in paragraph for phases 3 to 6

6.4.7 FDP_ITC.1 Import of user data without security attributes

FDP_ITC.1.1 The TSF shall enforce the [assignment: *access control SFP and/or information flow control SFP*] when importing user data, controlled under the SFP, from outside of the TSC.

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

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [assignment: *additional importation control rules*].

Iteration	access control SFP and/or information flow control SFP
UB0'_FDP_ITC01	**access control SFP (See FDP_ACF.1)**

Table 41 : Import of user data without security attributes

6.4.8 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 [selection: *allocation of the resource to*, *deallocation of the resource from*] the following objects: [assignment: *list of objects*].

Iteration	selection	list of objects
UB0'_FDP_RIP	deallocation of the resource from	On one side, the all memory reserved to processing tasks is reinitialized at the beginning of each session. On the other side, the memory containing sensitive data which may jeopardize a function dedicated to the security is also reinitialized between two functions

Table 42 : Subset residual information protection for B0'

6.4.9 FDP_SDI.2 Stored data integrity monitoring and action

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

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*].

Iteration	integrity errors	user data attributes	action to be taken
UB0'_FDP_SDI01	unintentional integrity errors due to Hardware errors	user data updating on E²PROM.	The Error status « EEPROM Failure » is returned to the terminal after unsuccessfuls tries of writting on EEPROM and the word is not validated on EEPROM.
UB0'_FDP_SDI02	Loss of integrity affecting E²PROM memories in reading E²PROM data	Data value read from EEPROM.	Mute card.

Table 43 : Stored data integrity monitoring and action for B0'

6.5 CLASS FIA IDENTIFICATION AND AUTHENTICATION

6.5.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TOE Security Functions shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TOE Security Functions shall [assignment: *list of actions*].

Iteration	Number	List of authentication events	List of actions
UB0'_FIA_AFL01	**3**	**Unsuccessful Holder authentication attempts since the last successful authentication**	**The application B0' becomes in Blocked state**
UB0'_FIA_AFL02	**1 or 2**	**Unsuccessful Holder authentication attempts since the last successful authentication**	**Block the Issuer authentication and the Delegation responsible for Issuer authentication.**
UB0'_FIA_AFL03	**1**	**Unsuccessful Issuer authentication attempts**	**The application B0' becomes in Blocked state.**
UB0'_FIA_AFL04	**1**	**Unsuccessful Delegation responsible for Issuer authentication attempts**	**The application B0' becomes in Blocked state.**

Table 44 : Authentication failure handling for B0'

6.5.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TOE Security Functions shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

Iteration	List of security attributes
UB0'_FIA_ATD	**'Role', 'Access conditions'**

Table 45 : User attribute definition in phase 7

6.5.3 FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

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

Iteration	List of TSF-mediated actions	Refinement
UB0'_FIA_UAU01	- Terminal Reads Static authentication of the Card,	**Card Holder authentication by the terminal**
UB0'_FIA_UAU02	- Read of Card manufacturing data	**Manufacturing data**
UB0'_FIA_UAU03	- Set up lock bits	**Pointer area**
UB0'_FIA_UAU04	- Certificate command in free reading area	**Cryptography**
UB0'_FIA_UAU05	- Write without validation in free/reserved access area (Word Not validated). - Free reading	**Read/Write access**

Table 46 : Authentication iterations for B0'

6.5.4 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.

6.5.5 FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment:*identified authentication mechanism(*s)].

Iteration	Identified authentication mechanism(s)
UB0'_FIA_UAU06	**Identified authentication mechanism(s) are in conformity with GIE CB specification - [SSAB0']**

Table 47 : Single-use authentication mechanisms iterations

6.5.6 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment: *list of 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 succesfully identified before allowing any other TSF-mediated actions on behalf of that user.

Iteration	List of TSF-mediated actions
UB0'_FIA_UID01	- Terminal Reads Static authentication of the Card holder,
UB0'_FIA_ UID02	- Read of Card manufacturing data.
UB0'_FIA_ UID03	- Set up lock bits
UB0'_FIA_ UID04	- Certificate command in free reading area
UB0'_FIA_ UID05	- Write without validation in free / reserved access area (Word Not validated). - Free reading

Table 48 : Identification refinement for B0'

6.5.7 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.

6.6 CLASS FMT : SECURITY MANAGEMENT

6.6.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

Iteration	selection: determine the behaviour of, disable, enable, modify the behaviour of	list of functions	the authorised identified roles
UB0'_FMT_MOF	**DISABLE**	**Autority authentication (Issuer, holder, Delegation responsible for issuer), Card authentication by certificate command, Transactions authentication.**	**Anybody by INVALIDATE COMMAND.**

Table 49 : Management of security functions behaviour for B0'

6.6.2 FMT_MTD.1 Management of TOE Security Functions data

FMT_MTD.1.1 The TOE Security Functions shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TOE Security Functions data*] to [assignment: *the authorised identified roles*].

Iteration	Selection	list of TOE Security Functions data	Authorised identified roles
UB0'_ FMT_MTD01	**Modify**	- **Key (fab,CO,CB)** - **PIN (More than ONCE)** -	**None**
UB0'_ FMT_MTD02	**Modify**	- **PIN (only ONCE)**	**Holder**

Table 50 : Management of TOE Security Functions data

6.7 CLASS FPR : PRIVACY

6.7.1 FPR_UNO.1 Unobservability*

FPR_UNO.1.1 The TOE Security Functions shall ensure that [assignment: *list of users and/or subjects*] are unable to observe the operation [assignment: *list of operations*] on [assignment: *list of objects*] by [assignment: *list of protected users and/or subjects*].

Iteration	list of users and/or subjects	list of operations	list of objects	list of protected users and/or subjects
UB0'_FPR_UNO	external users	- cryptographic operations, operations of comparison for authentication	user data	TOE

Table 51 : Unobservability

6.8 CLASS FPT : PROTECTION OF THE TOE SECURITY FUNCTIONS

6.8.1 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TOE Security Functions shall preserve a secure state when the following types of failures occur: [assignment: *list of types of failures in the TSF*].

Iteration	Refinement	list of types of failures in the TSF
UB0'_FPT_FLS01	**Configuration parameters**	**Inconsistent TSF data such as : PINs or Keys not initialized and B0' user mode.**
UB0'_FPT_FLS02	**Memory configuration**	**Inconsistent pointer No hierarchical pointer value**
UB0'_FPT_FLS03	**EEPROM Erasing data**	**Interruption in EEPROM erasing data**

Table 52 : Failure with preservation of secure state for B0'

6.8.2 FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: : *list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

Iteration	physical tampering scenarios	list of TSF devices/elements
UB0'_FPT_PHP0x	**Idem phases 3 to 6**	

Table 53 : Resistance to physical attack for B0'

See description in paragraph for phases 3 to 6

6.8.3 FPT_SEP.1 TOE Security Functions domain separation

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

FPT_SEP.1.2 The TOE Security Functions shall enforce separation between the security domains of subjects in the TOE Security Functions Scope of Control.

6.8.4 FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *list of TSF data types*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [assignment: *list of interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

Iteration	list of TSF data types	list of interpretation rules to be applied by the TSF
UB0'_FPT_TDC01	**Authentication data value,** **Pointers values consistency**	**GIE CB Specification**

Table 54 : Inter-TSF basic TSF data consistency

6.8.5 FPT_TST.1 TOE Security Functions testing

FPT_TST.1.1 The TOE Security Functions shall run a suite of self tests [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TOE Security Functions shall provide authorised users with the capability to verify the integrity of TOE Security Functions data.

This aspect of the functionality is not applicable: the integrity verification of TSF data stored on EEPROM is based on consistency of data, IC technology and EEPROM Stored data integrity monitor (defined in FDP_SDI.2).

FPT_TST.1.3 The TOE Security Functions shall provide authorised users with the capability to verify the integrity of stored TOE Security Functions executable code.

This aspect of the functionality is applicable for the executable code stored on EEPROM.

Iteration	Selection	Refinement
UB0'_FPT_TST	During initial start-up	Application start-up

Table 55 : Failure with preservation of secure state for B0'

7. TOE Security Assurance Requirements

The Assurance requirements is **EAL 4 augmented** with additional assurance components listed in this section for B0'.

Additional components are higher hierarchical to the components specified in EAL4.

The assurance requirements of this security target are summarized in the following table.

Requirement	Name	Type
EAL4	Methodically Designes, Tested and Reviewed	Assurance level
ADV_IMP.2	Implementation of the TSF	Higher hierarchical component
ALC_DVS.2	Sufficiency of security measures	Higher hierarchical component
AVA_VLA.4	Highly resistant	Higher hierarchical component

Table 56: **Additionale Security Asurance requirements (Complete)**

7.1 ADV_IMP.2 IMPLEMENTATION OF THE TSF

Developer action elements:

ADV_IMP.2.1D The developer shall provide the implementation representation for the entire TSF.

Content and presentation of evidence elements:

ADV_IMP.2.1C The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.

ADV_IMP.2.2C The implementation representation shall be internally consistent.

ADV_IMP.2.3C The implementation representation shall describe the relationships between all portions of the implementation.

Evaluator action elements:

ADV_IMP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_IMP.2.2E The evaluator shall determine that the implementation representation is an accurate and complete instantiation of the TOE security functional requirements.

7.2 ALC_DVS.2 SUFFICIENCY OF SECURITY MEASURES

Developer action elements:

ALC_DVS.2.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.2.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.2.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.2.3C The evidence shall justify that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

Evaluator action elements:

ALC_DVS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.2.2E The evaluator shall confirm that the security measures are being applied.

7.3 AVA_VLA.4 HIGHLY RESISTANT

Developer action elements:

AVA_VLA.4.1D The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.

AVA_VLA.4.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.4.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.3C The evidence shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.4C The analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

Evaluator action elements:

AVA_VLA.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.4.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

AVA_VLA.4.3E The evaluator shall perform an independent vulnerability analysis.

AVA_VLA.4.4E The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

AVA_VLA.4.5E The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a high attack potential.

8. TOE summary specification

The user authentication functions (FS2, FS3, FS4, FS5) use a probabilistic mechanism then these functions are SOF-high.

The application authentication function and the transaction authentication function (FS7 and FS8) use a cryptographic mechanism : The cryptographic mechanisms are not analyzed in AVA_SOF.1.

8.1 TOE SECURITY FUNCTIONS FOR B0'

FS1

INTEGRITE DES INFORMATIONS DE LA MEMOIRE

Intégrité des données de la mémoire utilisateur :

Pendant leur durée de vie, définie comme intervalle de temps entre deux écritures, modification ou effacement, borné par la durée de vie de la carte c'est-à-dire jusqu'à sa destruction par l'organisme émetteur, ce qui ne dépasse pas 10 ans, les données de la mémoire utilisateur ne subissent pas d'altération c'est-à-dire de changement non contrôlé d'état.

Intégrité des données de la mémoire de travail :

Pendant leur durée de vie, définie comme intervalle de temps entre deux écritures, modifications ou effacements, borné par la durée d'une SESSION, les données de la mémoire de travail ne subissent pas d'altération c'est-à-dire de changement non contrôlé d'état.

Intégrité des données de la mémoire programme :

Pendant leur durée de vie, définie comme intervalle de temps entre leur écriture et la destruction de la carte par l'organisme émetteur, ce qui ne dépasse pas 10 ans, les données de la mémoire programme ne subissent pas d'altération c'est-à-dire de changement non contrôlé d'état.

L'application B4-B0' ne reconnaît que 4 autorités, agréées par l'émetteur de la carte CB - l'encarteur (ou le personnalisateur), l'émetteur lui-même, le délégataire de l'émetteur et le porteur -, dont les droits ne peuvent être ouverts simultanément.

FS2

AUTHENTIFICATION DE L'ENCARTEUR (OU DU PERSONNALISATEUR)

C'est l'opération que l'utilisateur doit réaliser pour se faire reconnaître auprès de l'application B4-B0' comme l'encarteur (ou le personnalisateur) agréé par l'émetteur.

FS3

AUTHENTIFICATION DE L'EMETTEUR

C'est l'opération que l'utilisateur doit réaliser pour se faire reconnaître auprès de l'application B4-B0' comme l'émetteur lui-même.

FS4

AUTHENTIFICATION DU DELEGATAIRE DE L'EMETTEUR

C'est l'opération que l'utilisateur doit réaliser pour se faire reconnaître auprès de l'application B4-B0' comme le délégataire de l'émetteur.

FS5

AUTHENTIFICATION DU PORTEUR

C'est l'opération que l'utilisateur doit réaliser pour se faire reconnaître auprès de l'application B4-B0' comme le porteur.

FS7

AUTHENTIFICATION DE L'APPLICATION

C'est la fonction que l'utilisateur demande à l'application B4-B0' de réaliser afin de vérifier que les données d'identification sont présentes dans la mémoire utilisateur et conformes.

FS8

AUTHENTIFICATION (CERTIFICATION) DE LA TRANSACTION

C'est la fonction que l'utilisateur demande à l'application B4-B0' de réaliser afin de fournir la preuve que la transaction a bien été réalisée avec la carte CB identifiée.

FS9

INHIBITION DU MODE TESTS

A l'issue de la phase de fabrication, après une phase de tests du microcircuit programmé, le fonctionnement en mode tests du microcircuit programmé est inhibé de manière irréversible : les données (système ou utilisateur) sont entièrement sous le contrôle du système d'exploitation de la carte, que ce soit pour la lecture, l'écriture ou la modification.

Les tests effectués au cours de la phase de fabrication ne peuvent plus être utilisés.

FS10

CLOISONNEMENT DES ZONES DE MEMOIRE

· les données constituant la partie "logique" (programme exécutable) de l'application B4-B0' ne sont pas accessibles de l'extérieur, ni en lecture, ni en écriture, ni en modification, mais sont exécutables par le microcircuit électronique (MEMOIRE PROGRAMME),

· les données de travail transitoires, nécessaires au programme ainsi qu'à l'interface entre le programme et l'unité de traitement interne du microprocesseur, ne sont pas accessibles de l'extérieur, ni en lecture, ni en écriture, ni en modification, mais peuvent contenir des instructions exécutables à condition que celles-ci puissent être parfaitement identifiées par une simple étude du programme exécutable de l'application B4-B0' (MEMOIRE DE TRAVAIL),

· les données statiques applicatives sont accessibles par le monde extérieur, uniquement par l'intermédiaire de l'application B4-B0', au moyen du protocole d'échange de données conforme aux normes ISO (MEMOIRE DES DONNEES).

· La mémoire des données de la partie "données" de l'application B4-B0' est elle-même divisée en deux parties :

- l'une, secrète, non accessible de l'extérieur en lecture, écriture ou modification, contenant les données d'authentifications des autorités habilitées à exploiter l'application B4-B0' (MEMOIRE SECRETE),

- l'autre, accessible *en lecture, écriture ou modification comme précisé en Annexe A3 du document [SSAB0'] (ou Voir FDP_ACF.1 en phase 7)*, aux seules autorités habilitées à administrer la partie "données" de l'application B4-B0' (MEMOIRE UTILISATEUR).

FS11

PHASE D'UTILISATION

Durant la phase de personnalisation, la mémoire utilisateur est totalement subdivisée en zones auxquelles sont affectées sans ambiguïté des caractéristiques précisant si, durant la phase d'utilisation, l'accès à leurs ressources en lecture, écriture ou effacement sera :

· LIBRE, c'est-à-dire sans contrôle effectué par l'application B4-B0',

· RESERVE, c'est-à-dire limité à une ou plusieurs autorités - l'émetteur lui-même, le délégataire de l'émetteur ou le porteur - dont une authentification préalable sera requise par l'application B4-B0',

· INTERDIT, c'est-à-dire inaccessible par l'utilisateur.

L'accès peut être réservé indépendamment en lecture, écriture ou effacement.

Les zones d'accès de la mémoire utilisateur et la fonction de contrôle d'accès correspondante sont présentées en Annexe A3 *du document [SSAB0'] (ou Voir FDP_ACF.1 en phase 7)*.

FS12

ETAT DE BLOCAGE

En phase d'utilisation, mais dans un état de blocage, l'application B4-B0' interdit tout accès *en lecture ou lors de la validation en écriture* aux données de la mémoire utilisateur dont l'accès est interdit et à celles dont l'accès est réservé (cf. A3 *du document [SSAB0'] ou Voir FDP_ACF.1 en phase 7)*.

FS13

INVALIDATION

En cas d'invalidation du microcircuit programmé, l'application B4-B0' interdit de manière irréversible toute modification, écriture ou effacement de la mémoire utilisateur, mais rend l'accès libre en lecture à toutes les données dont l'accès était jusqu'alors réservé (cf. A3 *du document [SSAB0']* *ou Voir FDP_ACF.1 en phase 7*).

Les fonctions d'authentification des autorités (l'émetteur lui-même, le délégataire de l'émetteur ou le porteur), de la carte et des transactions sont désactivées.

FS14

IRREVERSIBILITE DES PHASES

L'application B4-B0' reconnaît les différentes phases de sa vie (configuration, utilisation ou invalidation), leur ordre chronologique et ne tolère aucun retour à une phase antérieure.

FS15

AUTORITE QUI A ECRIT

L'application B4-B0' enregistre, pour chaque mot de la mémoire utilisateur accessible en écriture, l'identité de l'autorité (le personnalisateur, l'émetteur lui-même, le délégataire de l'émetteur ou le porteur) qui écrit le mot (cf. A4 *du document [SSAB0']*).

FS16

AUTORITE QUI A BLOQUE

L'application B4-B0' enregistre et offre à l'utilisateur un moyen d'obtenir le type (émetteur ou porteur) de l'authentification infructueuse qui a provoqué le blocage.

FS17

LECTURE DES DONNEES EN PHASE D'UTILISATION

Lors de la lecture, par l'utilisateur, des données écrites dans la mémoire utilisateur réservées en écriture, l'application B4-B0' fournit l'identifiant de l'autorité qui les a écrites.

FS18

HYPERVISEUR DE SECURITE

Lors de la détection de conditions de fonctionnement ou d'environnement anormales, ou lors de la détection d'une incohérence des données de la mémoire utilisateur, l'application B4-B0' génère une action informative, corrective ou autoblocante.

FS19

LECTURE DES DONNEES EN PHASE D'INVALIDATION

En cas d'invalidation de l'application B4-B0', celle-ci rend l'accès libre en lecture *(suite à une validation en lecture : Voir spécifications DTE/SEC/SPE/1999-002 V3 commande Lecture page 47)* à toutes les données de la mémoire utilisateur dont l'accès était jusqu'alors réservé (cf. A3 *du document [SSAB0'] ou Voir FDP_ACF.1 en phase 7*).

FS20

REINITIALISATIONL'application B4-B0' réinitialise, d'une part lors de chaque début de session, la totalité des ressources de la mémoire de travail qui lui sont réservées, et d'autre part, entre deux fonctions, les ressources de sa mémoire de travail contenant des données sensibles susceptibles de mettre en péril une fonction dédiée à la sécurité.

FS21 DISPONIBILITE DES SERVICES RENDUS PAR LE MICROCIRCUIT PROGRAMME
En phase d'utilisation, les services et les ressources de l'application B4-B0' sont indisponibles si les données indiquant que la cible d'évaluation a été paramétrée (zones de la mémoire utilisateur), sont incohérentes ou ne sont pas validées, dans la mesure où l'application B4-B0' rend impossible tout accès à ses fonctionnalités.

8.2 ASSURANCE MEASURES BO' EAL4+

Requirement	Measures	Reference	Originator
ST	ST B0'		OCS
Configuration management			
ACM_AUT.1	Partial CM automation	- Manuel de gestion de configuration	OCS
ACM_CAP.4	Generation support and acceptance procedure	Manuel de gestion de configuration	OCS
ACM_SCP.2	Problem tracking CM coverage	- Manuel de gestion de configuration	OCS
Delivery and operation			
ADO_DEL.2	Detection of modification	-Procédures de livraison et de signature	OCS (Delivery of mask to STM)
ADO_IGS.1	Installation, generation and start-up procedures	- Procédure de création disquette STM -HOST/B0' mask option list for ST19SF02 chip -Procédure de pré-personnalisation - Documentation de livraison et de configuration B0'V3 - Démarrage et exploitation B0'V3	OCS GIE_CB GIE_CB
Development			
ADV_FSP.2	Fully defined external interfaces	-Spécification fonctionnelle du masque B0'V3 SRS/SECS	GIE_CB OCS specifs
ADV_HLD.2	Security enforcing high	SAD	OCS

Requirement	Measures	Reference	Originator
	level design		
ADV_LLD.1	Security enforcing low level design	SDD	OCS
ADV_IMP.2	Implementation of the TSF	Source	OCS
ADV_RCR.1	Informal correspondence demonstration	SRS/SAD/SDD	OCS
ADV_SPM.1	Informal TOE security policy model	Modèle de politique de sécurité B0'V3	OCS
Guidance document			
AGD_ADM.1	Administrator Guidance	- Documentation d'administration B0'V3	GIE_CB
AGD_USR.1	User guidance	-Spécification fonctionnelle du masque B0'V3 -Document d'utilisation B0'V3	GIE_CB GIE_CB
Life cycle support			
ALC_DVS.2	Sufficiency of security measures	Manuel de sécurité	OCS
ALC_LCD.1	Developer defined life-cycle model	Plan de développement	OCS
ALC_TAT.1	Well defined development tools	Fiche descriptive des outils utilisés	OCS
Tests			
ATE_COV.2	Analysis of coverage	STD	OCS
ATE_DPT.1	Testing high-level design	Mapping TSF/ SAD and tests	OCS
ATE_FUN.1	Functional testing	STD /STR	OCS
ATE_IND.2	Independent testing sample	Tests Platform and TOE	OCS
Vulnerability assessment			
AVA_MSU.2	Validation of guidance analysis	Facilité d'emploi	GIE_CB

Requirement	Measures	Reference	Originator
AVA_SOF.1	Strength of the TSF evaluation	Analyse de la résistance des mécanismes	OCS
AVA_VLA.4	Highly resistant : Construction vulnerability Usage vulnerability	Vulnérabilité en construction: Vulnérabilité en exploitation : B0' V3 security vulnerabilities and countermeasures	OCS GIE_CB

Table 57 : ST assurance measures

9. PP claims

This ST claims the PP/9911.

The ST19SF02ADxyz is compliant to the PP/9806.

9.1 PP REFERENCE

PP/9806 " Smart card Integrated Circuit " (V2.0 Issue September 1998)

PP/9911 "Smart card Integrated Circuit with embedded Software" (V2.0 Issue June 1999)

9.2 PP REFINEMENTS

The Application functions and environment are defined as [SSAB0'] compliant with the PP/9806 and PP/9911.

9.3 PP ADDITIONS

Additions of the FAU_GEN.1 and FAU_SAR.1 are mentioned in this ST to provide audit functions as defined in FS15, FS16 and FS17 of the [SSAB0'].

Addition of the FCO_NRO.1 is mentionned in this ST to provide payment transaction certificate as defined in FS8 of the [SSAB0'].

Additions of the FDP_IFF.1 and FDP_IFC.1 are mentioned in this ST to provide inhibition of critical test functionality and supports the non reversibility of the IC configuration functions as defined in FS9 of the [SSAB0'].

10. Rationale

This chapter is the OBERTHUR CARD SYSTEMS property.

11. Annex A

11.1 GLOSSARY

"CB" Abbreviation of "Cartes Bancaires" which qualifies, by extension, all what reffers to the Groupement des Cartes Bancaires interbancarity.

Dedicated Software Software part provided to test the component and/or to manage specific functions of the component.

IC designer Institution (or its agent) responsible for the IC development.

IC manufacturer Institution (or its agent) responsible for the IC manufacturing, testing, and pre-personalisation.

Integrated Circuit (IC) Electronic component(s) designed to perform processing and/or memory functions, which contains the following elemnts

- a logical arithmetic unit (ALU)
- a programmable, non programmable and non volatile memory
- an electronic memory, unaccessable from outside, required for internal processings of the B0' application and the ALU
- a programmable, re-programmable and non volatile memory, accessible from outside through an exhaustive set of commands

Interbancarity	Agreement the goal of which is to establish a total compatibility between the cards issued by all the French institutions for the payment (and the cash withdraw).
"Logical" part of:	set of organised and recognisable instructions executable by
- application	- the electronic chip processor
- Session	- time interval between two consecutive activations of B0' application
Personaliser	Institution (or its agent) responsible for the smartcard personalisation and final testing.
Smartcard	A credit/debit sized plastic card which has a non volatile memory and a processor unit embedded within it.
Smartcard embedded software developer	Institution (or its agent) responsible for the smartcard embedded software development and the specification of pre-personalisation requirements.
Smartcard issuer	Institution (or its agent) responsible for the smartcard product delivery to the smartcard end-user.
Smartcard product manufacturer	Institution (or its agent) responsible for the smartcard product finishing process and testing.

11.2 ABBREVIATION

IC : Integrated Circuit
POS : Point Of Sale
SFP : Security Fonction Policy
SP : Service Provider
TOE : Target Of Evaluation
TSC : Target of evaluation security functions Scope of Control
TSF : Target of evaluation Security Functions
TSP : Target of evaluation Security Policy