LOGIWAYS

Logiways TV Card

Public Security Target

Version 1.5 – October 15th, 2009

pure. sharp. powerful.

Document versions

Version	1.0
Date	March 17th, 2008
Written by	OPPIDA
Verified by	Michel MAILLARD
Approved by	Christian BÉNARDEAU
Comments	Document creation

Version	1.1
Date	August 28th, 2008
Written by	Michel MAILLARD
Verified by	Michel LUCAS
Approved by	Christian BÉNARDEAU
Comments	Changes according to SECAM_NOTE_02_v1.0 from SERMA

Version	1.2
Date	September 9th, 2008
Written by	Michel MAILLARD
Verified by	Michel LUCAS
Approved by	Christian BÉNARDEAU
Comments	Changes according to SECAM_NOTE_02_v2.0 from SERMA

Version	1.3
Date	April 30th, 2009
Written by	Michel MAILLARD
Verified by	Michel LUCAS
Approved by	Christian BÉNARDEAU
Comments	Changes according to SECAM_NOTE_05_v1.0 from SERMA

Version	1.4
Date	July 16th, 2009
Written by	Michel MAILLARD
Verified by	Michel LUCAS
Approved by	Christian BÉNARDEAU
Comments	Update to new Logiways template

Version	1.4L
Date	August 17th, 2009
Written by	Michel MAILLARD
Verified by	Michel LUCAS
Approved by	Christian BÉNARDEAU
Comments	Public version of the security target

Version	1.5
Date	October 15th, 2009
Written by	Michel MAILLARD
Verified by	Michel LUCAS
Approved by	Christian BÉNARDEAU
Comments	Update to new Logiways template

Foreword

Duplication of the present text is autorized by « Logiways », only if it respects the following points:

- ***Distribution free of charge,***
- ***No modification or alteration of this document,***
- ***Quotations must be easy to identify from their sources, e.g. "document origin from « Logiways »".***

Table of contents

Table of illustrations

Table of tables

Glossary

Name	Description
APDU	ISO 7816 elementary command
CW	Signal TV Descrambler Control Word
ECM	Exploitation message (CW transport and broadcasting features)
ECM_G	ECM Generator
EEPROM	Electronic Erasable Programmable Read Only Memory
EMM	Card access right management message
EMM_G	EMM Generator
HD	Hard disk for broadcast recording
RAM	Random Access memory
SAS	Subscriber Authorisation System
SMS	Subscriber Management System
ST7100	Hardware descrambler chip
STB	Set-Top Box
UA	Smart card serial number

1 Security Target Introduction

This document is the Security Target (ST) for the Common Criteria (CC) Evaluation of the LOGIWAYS TV Card for pay TV.

This introduction part is composed of the 4 following paragraphs:

- Paragraph 1.1 details references of the present document, the Security Target (ST),
- Paragraph 1.2 provides references of the target of evaluation (TOE),
- Paragraph 1.3 describes the TOE for future owner of the TOE who wants to check that it is well suited to his needs,
- Paragraph 1.4, is particularly suited for evaluators and certificators. It describes more precisely the TOE.

1.1 Security Target Reference

Title:	Logiways TV Cards Security Target
Version:	1.4
Writer:	Oppida on behalf of Logiways Team Reviews by Logiways Team
Reference:	LWSTVC-004-ST
Publication Date:	August 17th, 2009

1.2 Target of Evaluation Reference

Developer Name:	Logiways
Product Name:	Safe Access TV Cards
Product Version:	SafeAccess version 2.0 Release 67 on ST19NA18F IC Name : ST19NA18 external revision F Dedicated software : ZSD. Embedded software : NVB.
TOE Perimeter:	Smartcard Product for TV Access control implemented in accordance with LOGIWAYS AC card specifications.
Platform Targets:	Smartcard for use with Logiways STB only.

1.3 Target of Evaluation Overview

The Target of Evaluation (TOE) is the Smartcard Product for TV Access control implemented in accordance with LOGIWAYS AC card specification.

This smart card is compliant with TV operator requirements who want to market services in subscription mode, advance paid mode, and protect data recorded in a digital device such as a hard disk.

1.3.1 Type of TOE

The TOE type is a Smartcard product dedicated to pay TV system. It is aimed at providing to a customer access to digital broadcasts according to his television subscription.

1.3.2 TOE usage

The customer possesses a set-top box (STB) that descrambles television signals. This descrambler can possibly record some broadcasts into an integrated hard disk. System security is enhanced by the two following components working together:

- ST7100, descrambling signal TV component,
- Smart card, the TOE, that processes EMMs and ECMs in order to provide securely CWs to the ST7100 component.

A customer subscribes for a DVB-T television standard. The STB is in charge of decoding TV signals. Signals contain ciphered streams that can be deciphered by the smart card (TOE). Then, the TOE delivers the control words to the STB for deciphering.

The final customer is then provided access to television broadcasts according to his access rights.

1.3.3 TOE security features

Operator television broadcasts are transmitted scrambled in respect with DVB-T television standard. Control Words, hereafter designed CWs, allow descrambling and are renewed each 10 seconds approximately.

CWs are transmitted within TV streams, in secured messages that contain broadcast features such as broadcast date and service number. These messages, also called ECM, are transmitted to every access control descrambling equipment. The latter are only able to extract CWs with adequate secrets and rights they possess.

Access rights that permit access to operator broadcasts are transmitted in secured messages designated EMM. Access rights are renewed regularly for security reasons.

At the operator facilities, the SMS manages his customers in order to affect them dedicated access rights. The SAS makes up EMMs with input information provided by the SMS. The EMM_G device secures EMMs before they are broadcast.

The operator transmits access rights criteria to the ECM_G entity that builds and secures ECM before broadcasting.

The final customer possesses a set-top box. The STB descrambles television signals. This descrambler can possibly record some broadcasts into an integrated hard disk. System security is enhanced by the two following components working together:

- ST7100, descrambling signal TV component,
- Smart card, the TOE, that processes EMMs and ECMs in order to provide securely CWs to the ST7100 component.

The following figure provides an overview of the global system, with the TOE integration.

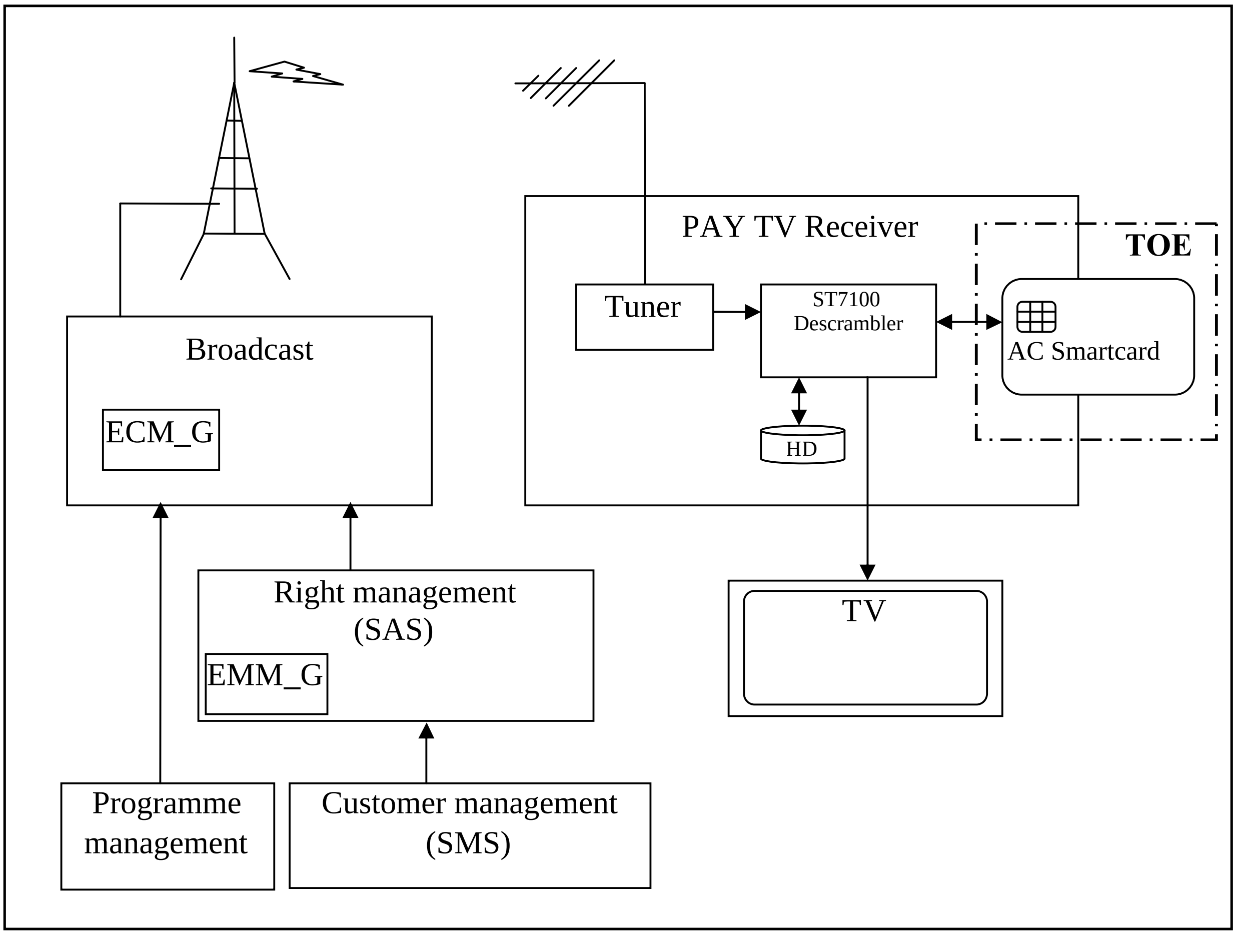

Figure 1 : General scheme

1.4 Target of Evaluation description

1.4.1 TOE presentation

The TOE is composed of the following and only parts:

- IC (Integrated Circuit) hardware,
- Dedicated software (System tools, Crypto library, Startup test),
- Application software (TV Access Control Software).

1.4.1.1 Integrated circuit hardware

This section describes the ST19NA18, a serial access microcontroller specially designed for cost-effective secure portable applications, member of the ST19N platform.

The TOE is a silicon chip with its Dedicated Software. The ST19NA18 is manufactured using an advanced highly reliable ST CMOS EEPROM submicron technology. The ST19N platform is based on the ST19W platform which comprises many already EAL5+ certified products.

The ST19NA18 offers even enhanced security functionalities and mechanisms. It is based on the ST Microelectronics 8-bit CPU already implemented on the ST19W product family and includes on-chip memories: User ROM, User RAM and EEPROM with state-of-the-art security features. ROM, RAM and EEPROM memories can be configured into partitions with customized access rules.

The CPU includes the Arithmetic Logic Unit (ALU), the control logic and registers available to the User. Access from any memory area to another is protected by 3 hardware firewalls, protecting memories, MAP and EDES. Access rules are user-defined and can be selected by mask options.

A specific logic block, named ’Security Administrator’, is added to the microcontroller to achieve an extremely high level of security against software and hardware attacks.

This device also includes two True Random Number Generators compliant with both FIPS 140-2 and AIS31.

An Enhanced DES accelerator is accessible via cryptographic software libraries located in ST ROM for symmetrical algorithms (DES, Triple DES computations and CBC mode). This module provides a mathematically proven protection against side channel attacks (SPA, DPA, EMA, DEMA, DFA).

To support efficiently Public Key cryptography, a Modular Arithmetic Processor (MAP) based on a 1088-bit processor architecture processes very efficiently modular arithmetic up to 2176 bits using Montgomery method, including modular exponentiation with or without CRT.
Two serial interfaces compatible with the ISO 7816-3 standard are available. The ISO Asynchronous Receiver Transmitter (IART) provides high speed serial data capability.

A CRC calculation accelerator block is also available and is directly accessible by the User.

High performance can be reached by using high speed internal clock frequency (up to 28 MHz).

To summarize, the ST19NA18 provides very powerful features for high level security:

- Die integrity,
- Glitch detector,
- Signal filtering,
- Memories scrambling,
- Power-on reset management,
- EEPROM flash programming,
- RAM destruction after POR and Reset,
- True Random Number Generator,
- Environment sensors,
- Firewall against unauthorized access to memories,
- Security administrator to manage security detector alerts including fault injection control,
- EEPROM memory integrity check,
- Code Signature mechanism,
- User ROM access protected area,
- Extra Security Control register.

1.4.1.2 IC dedicated software

The ST19NA18 includes in the ST ROM a Dedicated Software which comprises test capabilities (test operating system, called "autotest") and libraries (system ROM library and cryptographic library).

A software library provides additional primitives, including prime numbers generation up to 1088 bits, enabling the card to generate its own keys.

A software library supporting the Advanced Encryption Standard (AES). This module provides a mathematically proven protection against side channel attacks.

1.4.1.3 Smartcard embedded application software

The application software is developed by LOGIWAYS and is written in assembly language. It takes control of the card at the startup with the help of library in the dedicated software.

1.4.2 TOE life cycle

The Smart Card product life-cycle is decomposed into 7 phases, according to the “Smart Card Integrated Circuit Protection Profile” and is described in the following table

Phase		Description
Phase 1	Smartcard Embedded Software Development	The smartcard embedded software developer (LOGIWAYS) is in charge of the smartcard embedded software development and the specification of IC pre-personalisation requirements.
Phase 2	IC Development	The IC designer (ST Microelectronics) designs the IC, develops IC dedicated software, provides information, software or tools to the smartcard embedded software developer, and receives the smartcard embedded software from the developer, through trusted delivery and verification procedures. From the IC design, IC dedicated software and smartcard embedded software, he constructs the smartcard IC database, necessary for the IC photo mask fabrication.
Phase 3	IC Manufacturing and testing	The IC manufacturer (ST Microelectronics) is responsible for producing the IC through three main steps : IC manufacturing, IC testing and pre-personalisation.
Phase 4	IC Packaging and testing	The IC packaging manufacturer is responsible for the IC packaging and testing, personalisation.
Phase 5	Smartcard Product Finishing Process	The smartcard product manufacturer is responsible for the smartcard product finishing process and testing.
Phase 6	Smartcard Personalization	The personaliser is responsible for the smartcard final personalization and tests.
Phase 7	Smartcard End Usage	The smartcard issuer (LOGIWAYS) is responsible for the smartcard product delivery to the smartcard end-user, and the end of life process.

Table 1: Smartcard product life cycle

1.4.3 TOE Perimeter

1.4.3.1 TOE logical perimeter

The TOE logical perimeter is made of the dedicated software, which includes system tools, Crypto library, startup test, and the application software which is the TV access control software.

1.4.3.2 TOE physical perimeter

The TOE physical perimeter is made of the ST19NA18 chip, a serial access microcontroller specially designed for cost-effective secure portable applications, member of the ST19N platform. This chip is integrated into a ISO7816-1,2,3 smartcard standard. The smartcard is compliant with T=0 ISO7816 protocol.

1.4.4 TOE environment

Considering the TOE, five types of environment are defined:

- Development environment corresponding to phase 1 and 2,
- Production environment corresponding to phase 3 to 5,
- Personalization environment corresponding to phase 6,
- End-user environment corresponding to phase 7.

1.4.4.1 TOE development environment

1.4.4.1.1 Phase 1: Smartcard Embedded Software Development

To assure security, the environment in which the development takes place is made secure with controllable accesses having traceability.

The development begins with the TOE’s specification. 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.

Embedded software is delivered to IC manufacturing transported and worked in a secure environment.

All software developments are made by LogiWays engineers only (no subcontractor) in LogiWays premises located at 24-26 rue Louis ARMAND 75015 PARIS.

LOGIWAYS delivers the embedded software to ST ROUSSET responsible from hand to hand. During the transfer of sensitive data electronically, procedures are established to ensure that the data arrives only at the destination and are not accessible at intermediate stages (e.g. stored on a buffer server where system administrators make backup copies).

1.4.4.1.2 Phase 2: IC Development

The IC development environment is described in the PP/9806, section 2.3.1.

This description has been refined in the ST19NA18 Security Target to include industrial parameters whose definition is reproduced hereafter for reader's convenience. The development centers involved in the development of the TOE are the following:

- ST ROUSSET and ST ANG MO KIO, for the design activities,
- ST ROUSSET, for the engineering activities and for the software development activities.

1.4.4.2 TOE production environment

The production environment is described in the PP/9806, section 2.3.2.

1.4.4.2.1 Phase 3 IC Manufacturing and testing

This description has been refined in the ST19NA18 Security Target to include industrial parameters whose definition is reproduced hereafter for reader's convenience.

The authorized front-end plant actually involved in the manufacturing of the TOE is ST ROUSSET.

The authorized sub-contractor actually involved in the TOE mask manufacturing is DNP Japan.

The authorized EWS plant actually involved in the testing of the TOE is ST ROUSSET.

1.4.4.3 TOE-user environment

1.4.4.3.1 Phase 4 IC Packaging and testing

For security reasons, the processes of IC packaging and testing are done in a secure environment with adequate personnel, organizational and technical security measures.

1.4.4.3.2 Phase 5 Smartcard Product Finishing Process

Finishing process writes serial number to each TOE. For security reasons the processes of Smartcard Finishing Process are done in a secure environment with adequate personnel and organizational security measures.

1.4.4.3.3 Phase 6 Smartcard personalization

For security reasons, the processes of Smartcard personalization are done in a secure environment with adequate personnel and organizational security measures.

For technical security reasons the personalization messages are generated securely by crypto smartcard.

1.4.4.3.4 Phase 7 Smartcard usage

The TOE after its personalization is ready to be used in the customer's STB. In this insecure end-user environment, all security functions are active and cannot be disabled.

1.4.5 TOE logical phases

The logical phases available on the ST19NA18 by the dedicated software are:

- TEST configuration, then
- ISSUER configuration, then
- USER configuration.

During phases 4 to 7, the TOE shall be in USER configuration according to the developer request.

The logical phases available on the TOE by the application software are:

- Packaging configuration (Phase 5), then
- Personalization configuration (Phase 6), then
- Customer configuration (Phase 7).

1.4.6 TOE intended usage

This section describes the intended usage of the TOE during end-user phase 7.

The smartcard provide access control to MPEG multiplex of one or more broadcast services from pay TV channels.

For this, it grants to the smart card end-user:

- Access to services that the end user has subscribed,
- Access to broadcasting services recorded into the STB hard disk,

Access rights management ensures:

- Allocation, modification or suppression of individual access rights,
- Allocation, modification or suppression of user groups access rights,
- Banning or authorizing hard disk recording,
- STB and smart card pairing.

The TOE is compliant with the following functionalities:

- Protection of exploitation and management messages received by the STB,
- Protection of data exchanges with the STB,
- Protection of STB signal descrambling secrets,
- Protection of data stored into the hard disk,

- Protection against management messages replays,

- Protection of software updates.

External elements to the TOE are:

- The Set Top Box (STB) composed of :

    - Smart card reader integrated into the STB,
    - Exploitation system STB,
    - ST7100 component that descrambles signal.

- TV Signal broadcasting system composed of:

    - ECM exploitation messages generator,
    - EMM management messages generator.

2 Conformance claims

2.1 Common Criteria conformance

This Security Target (ST) claims to be conformant to the Common Criteria version 3.1:

- [1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 1, September 2006.
- [2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 3.1, Revision 2, September 2007.
- [3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 2, September 2007.

Furthermore, it claims to be CC Part 2 conformant and CC Part 3 conformant.

2.2 Protection Profile conformance

This Security Target (ST) claims to be conformant with the following protection profile:

- Smart Card Integrated Circuit with Embedded Software; Version 2.0, June 1999.

This Security Target also claims to be conformant with the Smart Card Integrated PP/9806 Version 2.0 Protection Profile.

Note : This Security Target is derived from PP/9911 adapted to Common Criteria v3.1 : choice of ADV_IMP.1 and ATE_DPT.2.

2.3 Package claim

The chosen level of assurance for the TOE is EAL4+, augmented with the components ALC_DVS.2, AVA_VAN.5.

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.

3.1 Assets

Assets are security relevant elements of the TOE that include:

- the IC specifications,
- the IC design,
- the development tools and technology,
- the IC Dedicated software.
- Smart Card Embedded Software Assets that include:
    - specifications,
    - implementation,
    - software (in ROM),
    - related documentation.
- Application Data of the TOE
    - system specific data such as Access rights, Access criteria, Control Word for deciphering service, Keys for data confidentiality and authentication, Updated software (in EEPROM),
    - initialization data,
    - pre-personalization requirements,
    - personalization data.

The TOE itself is therefore an asset.

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

3.1.1 TSF data

TSF data are data that are used by the TOE in order to enhance security.

TSF data are the following:

- CW encryption key for recording,
- CW encryption key for STB,
- APDU encryption key for STB,
- Management keys,
- Exploitation keys,
- Operator individual keys,
- Operator keys,
- XDCE and service diversifying parameter,
- EEPROM code,
- Encryption key for EEPROM data protection.

3.1.2 User data

User data are data that are manipulated by the TOE.

User data are the following:

- EMM,
- ECM,
- CW,
- Service access rights,
- Smartcard reference,
- Operator reference.

3.1.3 Essential services

Essential services offered by the TOE are the following:

- Authentication of EMM messages,
- Trusted channel,
- Authentication of ECM messages,
- Integrity control of ECM messages,
- Integrity control of EMM messages,
- Decryption of EMM messages,
- Decryption of ECM messages,
- Decryption of CW,
- Encryption of CW for STB,
- Encryption of CW for recording,
- Protection of secrets.

3.1.4 Security needs

Confidentiality, Integrity and Availability are the criteria used to describe security needs.

Security needs are expressed in the following table.

Assets	Security needs		
	Availability *	**Integrity**	**Confidentiality**
Services			
Authentication of EMM messages		X	
Trusted channel		X	X
Authentication of ECM messages		X	
Integrity control of ECM messages		X	
Integrity control of EMM messages		X	
Decryption of EMM messages		X	X
Decryption of ECM messages		X	X
Decryption of CW			X
Encryption of CW for STB			X
Encryption of CW for recording		X	X
User data			
EMM		X	X
ECM		X	X
CW		X	X
Service access rights	X	X	
Smartcard reference	X	X	
Operator reference	X	X	
TSF data			
Ciphering key for CW Recording		X	X
Ciphering key for CW STB encrypting		X	X
Management public key (authenticate EMM)		X	
Exploitation keys (decrypt ECM)	X	X	X
Management key (symmetric key, decrypt EMM)		X	X
Operator individual keys (decrypt EMM)		X	X
Public Operator key		X	
XDCE and service diversifying parameter		X	
EEPROM code		X	X

Table 2: Assets and security needs

* Availability is relevant to public and in-clear data seen from outside.

The following figure illustrates the TOE main functions in its end usage environment.

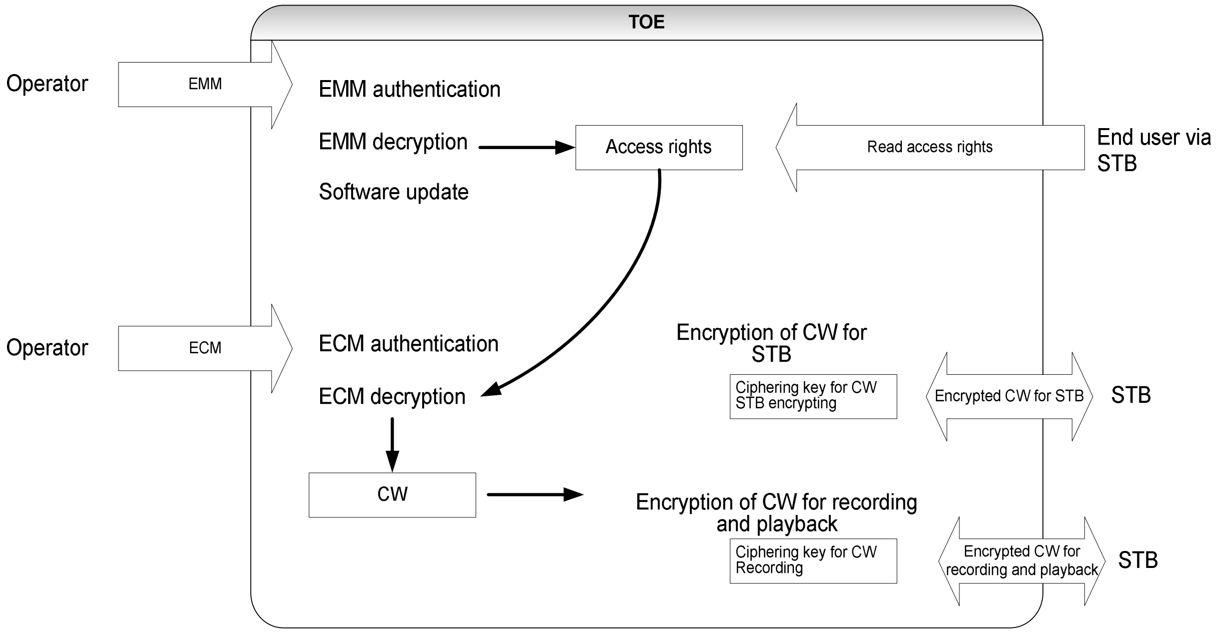

Figure 2: TOE functions in its end usage environment

3.2 Assumptions

Security always concerns the whole system: the weakest element of the chain determines the total system security. Assumptions are described in the following parts.

3.2.1 Assumptions on phase 1

(PP9911)

A.DEV_ORG

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.

3.2.2 Assumptions on the TOE delivery process (phases 4 to 7)

(PP9911)
Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives as described in the following assumptions:

A.DLV_PROTECT
Procedures shall ensure protection of TOE material/information under delivery and storage.

A.DLV_AUDIT
Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.

A.DLV_RESP
Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

3.2.3 Assumptions on phase 4 to 6

(PP9911)

A.USE_TEST
It is assumed that appropriate functionality testing of the TOE is used in phases 4, 5 and 6.

A.USE_PROD
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).

A.SECURE_PERSO
It is assumed that personalization phase permit secure personalization operations.

3.2.4 Assumptions on phase 7

A.USE_DIAG (PP9911)*

It is assumed that secure communication protocols and procedures are used between Smart Card and terminal.

A.STB

Descrambling control words from STB flows are protected against disclosure in the STB. Pairing and confidentiality keys are located in the STB and are protected against tampering and disclosure.

A.USE_ORG

It is assumed that physical protection, exploitation rules and access rights at the service streaming facilities are respected, especially regarding password, ECM ciphering units, smartcard).

It is assumed that physical protection, exploitation rules and access rights at the operator facilities are respected, especially regarding password, EMM ciphering units, smartcard, and subscriber management software.

A.USE_RENEWAL

Service access rights are renewed at least monthly. Service CWs are renewed each 10 seconds approximately.

3.3 Threats

3.3.1 General Threats of Smartcard Embedded Software

General 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).

Unauthorized full or partial cloning of the TOE

T.CLON*

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

Threats on phase 1

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

a) Threats on the Smart Cards 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 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.

T.DIS_INFO*
(Type b)

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.

T.DIS_DEL*
(Type c)

Unauthorized disclosure of the Smart Card Embedded Software and any additional application data (such as IC pre-personalization requirements) during the delivery to the IC designer.

T.DIS_ES1
(Type a)

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).

T.DIS_TEST_ES
(Type a and c)

Unauthorized disclosure of the Smart Card ES test programs or any related information.

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.

T.T_DEL*
(Type c)

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.

T.T_TOOLS
(Type a and b)

Theft or unauthorized use of the Smart Card ES development tools (such as PC, development software, data bases).

T.T_SAMPLE2
(Type a)

Theft or unauthorized use of TOE samples (e.g. bond-out chips with the Embedded Software).

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 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 implementation of malicious Trojan horses.

T_MOD_DEL*
(Type c)

Unauthorized modification of the Smart Card Embedded Software and any additional application data (such as IC prepersonalization requirements) during the delivery process to the IC designer.

T.MOD
(Type a)

Unauthorized modification of ES and/or Application Data or any related information (technical specifications).

Threats on delivery for/from phase 1 to phases 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:

T.DIS_DEL1

Unauthorized disclosure of Application Data during delivery to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.

T.DIS_DEL2

Unauthorized disclosure of Application Data delivered to the IC Packaging manufacturer, he Finishing process manufacturer or the Personalizer.

T.MOD_DEL1

Unauthorized modification of Application Data during delivery to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.

T.MOD_DEL2

Unauthorized modification of Application Data delivered to the IC Packaging manufacturer, the Finishing process manufacturer or the Personalizer.

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.

T.DIS_ES2

Unauthorized disclosure of ES and Application Data (such as data protection systems, memory partitioning, cryptographic programs and keys).

Theft or unauthorized use of assets

Potential attackers may gain access to the TOE and perform operation 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

T.T_ES

Theft or unauthorized use of TOE (e.g. bound out chips with embedded software).

T.T_CMD

Unauthorized use of instructions or commands or sequence of commands sent to the TOE.

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

T.MOD_LOAD

Unauthorized loading of programs.

T.MOD_EXE

Unauthorized execution of programs.

T.MOD_SHARE

Unauthorized modification of program behavior by interaction of different programs.

T.MOD_SOFT*

Unauthorized modification of Smart Card Embedded Software and Application Data.

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	Phase1	Phase 4	Phase 5	Phase 6	Phase 7
T.CLON*	Class II	Class I	Class I	Class I	Class I
T.DIS_INFO*	Class II				
T.DIS_DEL*	Class II				
T.DIS_DEL1	Class II				
T.DIS_DEL2		Class II	Class II	Class II	
T.DIS_ES1	Class II				
T.DIS_TEST_ES	Class II				
T.DIS_ES2		Class I	Class I	Class I	Class I
T.T_DEL*	Class II				
T.T_TOOLS	Class II				
T.T_SAMPLE2	Class II				
T.T_ES		Class I	Class I	Class I	Class I
T.T_CMD		Class I	Class I	Class I	Class I
T.MOD_DEL*	Class II				
T.MOD_DEL1	Class II				
T.MOD_DEL2		Class II	Class	II	
T.MOD	Class II				
T.MOD_SOFT*		Class I	Class I	Class I	Class I
T.MOD_LOAD		Class I	Class I	Class I	Class I
T.MOD_EXE		Class I	Class I	Class I	Class I
T.MOD_SHARE		Class I	Class I	Class I	Class I

Table 3: Relationship between phases and threats

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

3.3.2 TOE specific threats on phase 7

Specific threats that can compromise TOE security are:

T.RIGHT_MOD

This threat deals with an unauthorized modification or creation of customer rights into the TOE.

T.KEY_DIS

This threat deals with an unauthorized disclosure of keys during their transfer to the TOE.

T.AC_MOD

This threats deals with an unauthorized modification of entitlement control message.

T.STB_ABUSE

This threat deals with an unauthorized use of the TOE. A malicious customer tries to use his smartcard with an unauthorized equipment such as another terminal.

T.RECORD_ABUSE

This threat deals with an unauthorized use of the TOE. A malicious customer, with his own smartcard, tries to access to a video and audio stream that was recorded by another customer.

T.UPDATE_MOD

This threat deals with an unauthorized use, modification or creation of software update. A malicious user tries to upload a software update with a Trojan horse into the TOE.

T.UPDATE_LOCK

This threat deals with an unauthorized blocking of software update.

T.REPLAY

This threat deals with an unauthorized use of obsolete message.

3.4 Organisational Security Policies

The TOE security objectives are derived purely from threats and assumptions therefore this section has been omitted.

4 Security objectives

4.1 Security objectives for the TOE

4.1.1 General Security Objectives

O.TAMPER_ES

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.

O.CLON*

The TOE functionality must be protected from cloning.

O.OPERATE*

The TOE must ensure continued correct operation of its security functions.

O.FLAW*

The TOE must not contain flaws in design, implementation or operation.

O.DIS_MECHANISM2

The TOE shall ensure that the ES security mechanisms are protected against unauthorized disclosure.

O.DIS_MEMORY*

The TOE shall ensure that sensitive information stored in memories is protected against unauthorized disclosure.

O.MOD_MEMORY*

The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification.

4.1.2 TV Card Security Objectives

O.DATA_WRITE

The TOE must limit data write access to confidential and authenticated EMM (Entitlement Management Message) of the operators and the manager.

O.SECURE_ENTITLEMENT

The TOE shall use secure protocol for transmission of ECM (Entitlement Control Message).

O.STB_PAIRING

STB and TOE shall be paired before being used.

O.SECURE_RECORD

The TOE shall use secure protocol to protect the data write on external media.

O.SECURE_UPDATE

The TOE shall not permit loading or executing of unauthorized Update Software.

O.UPDATE_VERSION

The TOE shall use protocol to control Software update versioning.

O.INDEX

The TOE shall use protocol to control message sequence.

4.2 Security Objectives for the environment

4.2.1 Objectives on phase 1

OE.DEV_TOOLS*

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 in the integrity of program and data.

OE.DEV_DIS_ES

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.

It must be ensured that tools are only delivered and accessible 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.

OE.SOFT_DLV*

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.

OE.INIT_ACS

Initialization Data shall be accessible only by authorized personnel (physical, personnel, organizational, technical procedures).

OE.SAMPLE_ACS

Samples used to run tests shall be accessible only by authorized personnel.

4.2.2 Objectives on the TOE delivery process (phases 4 to 7)

OE.DLV_PROTECT*

Procedures shall ensure protection of TOE material/information under delivery including the following objectives:

- non-disclosure of any security relevant information,
- identification of the element under delivery,
- meet confidentiality rules (confidentiality level, transmittal form, reception acknowledgment),
- physical protection to prevent external damage,
- secure storage and handling procedures (including rejected TOE's),
- traceability of TOE during delivery including the following parameters:
  - origin and shipment details,
  - reception, reception acknowledgement,

- location material/information.

OE.DLV_AUDIT*

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.

OE.DLV_RESP*

Procedures 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.

4.2.3 Objectives on delivery from phase 1 to phases 4, 5 and 6

OE.DLV_DATA

The Application Data must be delivered from the Smart Card embedded software developer (phase 1) either to the IC Packaging manufacturer, the Finishing Process manufacturer or the Personalizer through a trusted delivery and verification procedure that shall be able to maintain the integrity and confidentiality of the Application Data.

4.2.4 Objectives on phases 4 to 6

OE.TEST_OPERATE*

Appropriate functionality testing of the TOE shall be used in phases 4 to 6. During all manufacturing and test operations, security procedures shall be used through phases 4, 5 and 6 to maintain confidentiality and integrity of the TOE and its manufacturing and test data.

OE.SECURE_PERSO

The personalization operations in phases 4 to 6 shall be performed along procedures that shall ensure that people dealing with the personalization operations have got the required skill, training, knowledge and tools to meet trustfully the personalization requirements defined by the embedded software developer.

4.2.5 Objectives on phase 7

OE.USE_DIAG*

Secure communication protocols and procedures shall be used between the Smart Card and the terminal.

OE.STB

Descrambling control words must be deciphered only in the STB flow descrambling circuit (these CW must not be stored in clear into the STB). Pairing and confidentiality keys located into the STB must be protected for confidentiality and integrity.

OE.USE_ORG

Only authorized personnel have access to tools in charge of EMM and ECM secure message generation. Secure message generators use specific crypto smartcards to generate management and exploitation messages. Specific crypto smartcards are accessible only to authorized personnel.

Crypto smartcards that are not in use must be physically stored in secure areas.

OE.USE_RENEWAL

Access rights to the TV service must be renewed monthly. Ciphering key (CWs) must change each 10 seconds aproximately.

5 Security Requirements

5.1 Security Functional Requirements for the IT environment

This chapter defines the functional requirements for the TOE IT environment.

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 STB] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [APDU exchange].

Note: The trusted channel protects the channel data from modification and disclosure.
Note: In this functional requirement, the "TSF" is the STB.

5.2 TOE Security Functional Requirements

This chapter defines the functional requirements for the TOE smartcard embedded software using all functional requirements components drawn from the PP9911 protection profile.

Requirements	Title
FAU_SAA.1	Potential violation analysis
FCS_CKM.3/ECM/EMM	Cryptographic key access
FCS_CKM.3/STB_MESS	Cryptographic key access
FCS_CKM.3/AUTH	Cryptographic key access
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/ECM_EMM	Cryptographic operation
FCS_COP.1/STB_MESS	Cryptographic operation
FCS_COP.1/AUTH	Cryptographic operation
FCS_COP.1/HASH	Cryptographic operation
FDP_ACC.2/EMM&ECM	Complete access control
FDP_ACF.1/EMM&ECM	Security attribute based access control
FDP_DAU.1/EMM&ECM	Basic Data Authentication
FDP_ETC.1/CW export	Export of user data without security attributes
FDP_IFC.1/CW export	Subset information flow control
FDP_IFF.1/CW	Simple security attributes
FDP_ITC.1/ECM&EMM	Import of user data without security attributes
FDP_RIP.1	Subset residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
FIA_AFL.1	Authentication failure handling
FIA_ATD.1/OPERATOR	User attribute definition

(to be continued next page)

FIA_ATD.1/STB	User attribute definition
FIA_UAU.1/STB	Timing of authentication
FIA_UAU.2/Operator	User authentication before any action
FIA_UAU.3/Operator	Unforgeable authentication
FIA_UAU.4	Single-use authentication mechanisms
FIA_UID.1/STB	Timing of identification
FIA_UID.2/Operator	User identification before any action
FIA_USB.1	User-subject binding
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPR_UNO.1	Unobservability
FPT_FLS.1	Failure with preservation of secure state
FPT_PHP.3	Resistance to physical attack
FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_TST.1	TSF testing
FTP_ITC.1	Inter-TSF trusted channel

Table 4: SFR synthesis

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 enforcement of the SFRs.

FAU_SAA.1.2: The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [Self test error, Stored data integrity error, Data input integrity error, Data input syntax error, Software or hardware failure] known to indicate a potential security violation;
b) [None].

FCS_CKM.3/ECM_EMM: Cryptographic key access

FCS_CKM.3.1: The TSF shall perform [the access to a key for the decryption of EMM & ECM] in accordance with a specified cryptographic key access method [access to the key by its reference depending on the type of message and on the operator reference] that meets the following: [Logiways Specific MSD_FILLE document].

FCS_CKM.3/STB_MESS: Cryptographic key access

FCS_CKM.3.1: The TSF shall perform [the access to a key for the encryption/decryption of the STB message] in accordance with a specified cryptographic key access method [access to the key by its reference depending on the type of message] that meets the following: [Logiways Specific MSD_FILLE document].

FCS_CKM.3/AUTH: Cryptographic key access

FCS_CKM.3.1: The TSF shall perform [the access to a key for the authentication of EMM, ECM and EEPROM code] in accordance with a specified cryptographic key access method [access to the key by its reference depending on the type of message] that meets the following: [Logiways Specific MSD_FILLE document].

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 [erasing keys by overwriting with random bytes] that meets the following: [Logiways Specific MSD_FILLE document].

FCS_COP.1/ECM_EMM: ECM/EMM cryptographic operation

FCS_COP.1.1: The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [symmetric algorithm] and cryptographic key sizes [of fixed length] that meet the following: [Logiways Specific GEN_CHIFF document].
Note: a symmetric algorithm is used to decipher ECM, EMM, CW and to cipher CW.

FCS_COP.1/STB_MESS : STB message cryptographic operation

FCS_COP.1.1: The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [symmetric algorithm] and cryptographic key sizes [of fixed length] that meet the following: [Logiways Specific GEN_CHIFF document].
Note: a symmetric algorithm is used to cipher and decipher APDU, CW and keys stored in EEPROM.

FCS_COP.1/AUTH: Authentication cryptographic operation

FCS_COP.1.1: The TSF shall perform [decryption] in accordance with a specified cryptographic algorithm [private/public keys algorithm] and cryptographic key sizes [of varying length] that meet the following: [Logiways Specific GEN_CHIFF document].
Note: a private/public key algorithm is used to authenticate ECM, EMM and EEPROM code.

FCS_COP.1/HASH: Hash cryptographic operation

FCS_COP.1.1: The TSF shall perform [hashing] in accordance with a specified cryptographic algorithm [SHA] and cryptographic key sizes [of varying length] that meet the following: [Logiways Specific GEN_CHIFF document].
Note: different algorithms are used for APDU and recorded CW hashing on one hand, for EMM, ECM and EEPROM code.

FDP_ACC.2/EMM&ECM: Complete access control

FDP_ACC.2.1: The TSF shall enforce the [EMM&ECM import policy] on [ECM & EMM messages] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2: The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1/EMM&ECM: Security attribute based access control

FDP_ACF.1.1: The TSF shall enforce the [ECM & EMM import policy] to objects based on the following: [Operation: EMM&ECM decryption
Object: EMM&ECM (attributes: operator references-), Rights (attributes: operator keys).].

FDP_ACF.1.2: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [if Rights allow it].

FDP_ACF.1.3: The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [None].

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

FDP_DAU.1/EMM&ECM: 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 [EMM & ECM messages].

FDP_DAU.1.2: The TSF shall provide [the smartcard] with the ability to verify evidence of the validity of the indicated information.

FDP_ETC.1/CW export: Export of user data without security attributes

FDP_ETC.1.1: The TSF shall enforce the [CW export policy] when exporting user data, controlled under the SFP(s), outside of the TOE.

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

FDP_IFC.1/CW export: Subset information flow control

FDP_IFC.1.1: The TSF shall enforce the [CW export policy] on [CW].

FDP_IFF.1/CW export: Simple security attributes

FDP_IFF.1.1: The TSF shall enforce the [CW export policy] based on the following types of subject and information security attributes: [Object :CW (attribute : encrypted)].

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: [CW is exported only when its attribute is “encrypted”].

FDP_IFF.1.3: The TSF shall enforce the [no additional rules].

FDP_IFF.1.4: The TSF shall explicitly authorise an information flow based on the following rules: [CW is encrypted].

FDP_IFF.1.5: The TSF shall explicitly deny an information flow based on the following rules: [CW is not encrypted].

FDP_ITC.1/ECM&EMM: Import of user data without security attributes

FDP_ITC.1.1: The TSF shall enforce the [ECM&EMM import policy] when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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 from] the following objects: [public keys, secret keys].

FDP_SDI.2: Stored data integrity monitoring and action

FDP_SDI.2.1: The TSF shall monitor user data stored in containers controlled by the TSF for [integrity errors] on all objects, based on the following attributes: [CRC, Hash].

FDP_SDI.2.2: Upon detection of a data integrity error, the TSF shall [temporarily lock the card].

FIA_AFL.1: Authentication failure handling

FIA_AFL.1.1: The TSF shall detect when [one] unsuccessful authentication attempts occur related to [EMM & ECM messages authentication].

FIA_AFL.1.2: When the defined number of unsuccessful authentication attempts has been [met or surpassed], the TSF shall [reject the message].

FIA_ATD.1/OPERATOR: User attribute definition

FIA_ATD.1.1: The TSF shall maintain the following list of security attributes belonging to individual users: [Operator keys].

FIA_ATD.1/STB: User attribute definition

FIA_ATD.1.1: The TSF shall maintain the following list of security attributes belonging to individual users: [STB message and ECM/EMM keys].

FIA_UAU.1/STB: Timing of authentication

FIA_UAU.1.1: The TSF shall allow [READING: Fab serial number (initialized by hardware manufacturer), Smartcard unique address (UA), Card manager data (Identification), Operators data (Identification)] 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.

FIA_UAU.2/Operator: User authentication before any action

FIA_UAU.2.1: The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.3/Operator: 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.

FIA_UAU.4: Single-use authentication mechanisms

FIA_UAU.4.1: The TSF shall prevent reuse of authentication data related to [EMM & ECM messages authentication].

FIA_UID.1/STB: Timing of identification

FIA_UID.1.1: The TSF shall allow [READING: Fab serial number (initialized by hardware manufacturer), Smartcard unique address (UA), Card manager data (Identification), Operators data (Identification)] 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.

FIA_UID.2/Operator: User identification before any action

FIA_UID.2.1: The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1: User-subject binding

FIA_USB.1.1: The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [STB message and ECM/EMM keys].

FIA_USB.1.2: The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [special EMM transmission that maps the STB message and ECM/EMM keys with the TOE].

FIA_USB.1.3: The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [no rules for the changing of attributes].

Note : Change of the STB message key is not managed by the TOE.

FMT_MOF.1: Management of security functions behaviour

FMT_MOF.1.1: The TSF shall restrict the ability to [modify the behaviour of] the functions [all functions] to [the operator].

Note: Modification of functions is realized by applicative code update (patch in EEPROM).

FMT_MSA.1: Management of security attributes

FMT_MSA.1.1: The TSF shall enforce the [EMM & ECM import policy] to restrict the ability to [change_default, query, modify, delete] the security attributes [user individual access rights attribute] to [the operator].

FMT_MSA.2: Secure security attributes

FMT_MSA.2.1: The TSF shall ensure that only secure values are accepted for [user individual access rights attribute].

FMT_MSA.3: Static attributes initialisation

FMT_MSA.3.1: The TSF shall enforce the [EMM & ECM import policy] to provide [temporary] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2: The TSF shall allow the [no identified authorized roles] to specify alternative initial values to override the default values when an object or information is created.

Note: User access rights (security attributes) are provided temporarily during initial client subscription.

FMT_MTD.1: Management of TSF data

FMT_MTD.1.1: The TSF shall restrict the ability to [modify] the [keys and EEPROM code] to [the manager].

FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [update of the EEPROM code].

FMT_SMR.1: Security roles

FMT_SMR.1.1: The TSF shall maintain the roles [STB, Operator, Manager].

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

FPR_UNO.1: Unobservability

FPR_UNO.1.1: The TSF shall ensure that [card holders] are unable to observe the operation [management and computation] on [TSF and user data] by [STB and operators].

Refinement: Here, unobservability means impossibility to obtain the address and / or the value of information during an operation on this information

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: [Failure detected by the hardware, Reset, Protocol error, Software failure detection].

FPT_PHP.3: Resistance to physical attack

FPT_PHP.3.1: The TSF shall resist [fault injection tampering] to the [TSF resources] by responding automatically such that the SFRs are always enforced.

FPT_TDC.1: Inter-TSF basic TSF data consistency

FPT_TDC.1.1: The TSF shall provide the capability to consistently interpret [CW encryption keys used for STB and recording] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2: The TSF shall use [message deciphering and HASH integrity] when interpreting the TSF data from another trusted IT product.

Note: the STB is considered as a trusted IT product.

FPT_TST.1: TSF testing

FPT_TST.1.1: The TSF shall run a suite of self tests [during initial startup] to demonstrate the correct operation of [the TSF].

FPT_TST.1.2: The TSF shall provide authorised users with the capability to verify the integrity of [TSF data].

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

Refinement: The TSF capability to verify the integrity is restricted to:

- *the integrity of TSF data stored in EEPROM (integrity check enforced by the TSF whenever the data is to be used)*
- *the integrity of the updated code, i.e. the code patch in EEPROM (integrity check enforced by the TSF when the patch is loaded)*

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another 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 STB] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [APDU exchange].

Note: The trusted channel protects the channel data from modification and disclosure.

5.3 TOE Security Assurance Requirements

The ST is conformant to a pre-defined named assurance package as follows:

EAL 4 augmented with AVA_VAN.5 Advanced methodical vulnerability analysis and ALC_DVS.2 Sufficiency of security measures components.

6 TOE summary specifications

Rationale between security features and security functional requirements are provided at the end of each security feature.

6.1 Head End Message

SF.HD_ACI: Head End Message Authentication, Confidentiality and Integrity

This security feature permits to ensure that the message has been generated and secured by an exploitation/management user. It verifies the authenticity of exploitation and management message using variable-length public keys. It decrypts exploitation and management messages to extract confidential data necessary to the smartcard for access to service (decryption uses a symmetric algorithm). Message integrity is also controlled (HASH algorithm).

FCS_CKM.3/ECM/EMM> Access to a key is done to ensure FCS_COP.1 operation.
FCS_CKM.3/AUTH> Access to a key is done to ensure FCS_COP.1 operation.
FCS_COP.1/ECM/EMM> Cryptographic operations : decryption using symmetric algorithm is used to access EMM and ECM messages.
FCS_COP.1/AUTH> Cryptographic operations; a private/public key algorithm is used to authenticate messages.
FCS_COP.1/HASH> Cryptographic operations; a hash algorithm is used to hash messages.
FDP_ACC.2/EMM&ECM; FDP_ACF.1/EMM&ECM > EMM & ECM import policy to use and manage access rights.
FDP_DAU.1/EMM&ECM> Verification of the validity of EMM and ECM (authentication).
FDP_ITC.1/ECM&EMM> Import of EMM and ECM messages.
FIA_ATD.1/OPERATOR> Operator public key is used to verify integrity of EMM and ECM.
FIA_UAU.2/Operator> The operator is successfully authenticated before allowing him to perform actions on the smartcard.
FMT_MSA.1> Only the operator is allowed to manipulate ECM&EMM message and modify access rights.
FMT_MSA.2> Only secure values are accepted for user rights.
FMT_MSA.3> Temporary access rights are transmitted through EMM by the operator.

6.2 STB Secure Channel Data Exchange

SF.STB_CI : STB Exchange Confidentiality and Integrity

This security feature protects data exchanged between the STB and the smartcard against tapping and disclosure. It also protects against use of non authorized STB and data injection into the smartcard. It establishes a secure channel between the STB and the smartcard after ensuring that the STB is the right one known from the operator. It crypts and decrypts data exchanged between the STB and the smartcard using a symmetric algorithm and fixed-length keys. It protects messages exchanged against existing modification messages with a hash.

FCS_CKM.3/STB_MESS> Access to a key is done to ensure FCS_COP.1 operation.
FCS_COP.1/STB_MESS> Cryptographic operation : encryption using a symmetric algorithm is used to protect data exchanged between STB and the smartcard.
FCS_COP.1/HASH> Cryptographic operations : a hash algorithm is used to hash messages.
FTP_ITC.1>Inter-TSF trusted channel (between STB and smartcard).
FIA_ATD.1/STB> STB key is used by a couple STB-Smartcard to crypt/decrypt CW
FIA_UAU.1/STB> Some information can be read by the end user, i.e. the customer, before the STB is authenticated.
FIA_UID.1/STB> Only a restricted set of information can be read by the an attacker; i.e. smartcard UA and operator reference.
FIA_USB.1> Smartcard and STB are paired through a special EMM message and with a key loaded into the STB.
FMT_SMR.1> Two roles are defined to allow EMM&ECM operations through a secure channel between STB and smartcard.

6.3 TV Signal descrambling Key Protection

SF.CW_CONF : Control Word Confidentiality

This security feature protects control words that permit to decrypt TV signal during transmission with the STB. It crypts control words using a fixed-length key and a symmetric algorithm. This key is related to each STB decrypting component.

FCS_CKM.3/STB_MESS> Access to a key is done to ensure FCS_COP.1 operation.
FCS_COP.1/STB_MESS> Cryptographic operations : encryption using a symmetric algorithm is used to protect data exchanged between STB and the smartcard.
FDP_ETC.1/CW export> CW word are exported outside the smartcard.
FDP_IFC.1/CW export, FDP_IFF.1/CW > CW are controlled before being exported; they are never exported in clear and are transmitted ciphered.
FIA_ATD.1/STB> STB key is used by a couple STB-Smartcard to crypt/decrypt CW.
FMT_SMR.1> Two roles are defined to allow correct ECM operations.

SF.CW_DESCR: Control Word Deciphering

This security feature decrypts control words extracted from ECM. It decrypts using a symmetric algorithm and a fixed-length exploitation key. This key is diversified by XDCE and service parameters.

FCS_CKM.3/ECM_EMM> Access to a key is done to ensure FCS_COP.1 operation.
FCS_COP.1/ECM_EMM> Cryptographic operations : decryption using a symmetric algorithm is used to access CW in ECM messages.

6.4 Recorded TV signal Protection

SF.REC_CI : Hard disk Recorded Data Confidentiality and Integrity

This security functionality protects messages used for recording TV broadcast into the hard disk (containing control words). It uses fixed-length keys, and symmatric encryption / decryption algorithms. It also uses a hash algorithm for integrity control.

FCS_CKM.3/STB_MESS> Access to a key is done to ensure FCS_COP.1 operation.
FCS_CKM.3/ECM_EMM> Access to a key is done to ensure FCS_COP.1 operation.
FCS_COP.1/STB_MESS> Cryptographic operations : encryption and decryption using a symmetrical algorithm are used in recorded messages.
FCS_COP.1/ECM_EMM> Cryptographic operations : encryption and decryption using a symmetrical algorithm are used in recorded messages.
FCS_COP.1/HASH> Cryptographic operations : a hash algorithm is used to hash messages.
FDP_ETC.1/CW export> CW word are exported outside the smartcard.
FDP_IFC.1/CW export, FDP_IFF.1/CW > CW are controlled before being exported; they are never exported in clear and are transmitted ciphered.
FIA_ATD.1/STB> STB key is used by a couple STB-Smartcard to crypt/decrypt CW.
FMT_SMR.1> Two roles are defined to allow correct EMM&ECM operations.
FPT_TDC.1> CW are decrypted by the TOE when imported from the STB (case of control words for a broadcast stream recorded into the internal hard disk).

6.5 Object Reuse

SF.HD_INDEX: Head End Message Index

This security feature protects the smartcard against old message replay attacks. This optional functionality is used only to protect critical messages, e.g. messages used to add rights to a customer. It ensures itself for correct management message broadcast sequence.

FIA_UAU.3/Operator> The smartcard rejects messages that have not been successfully authenticated.
FIA_UAU.4> The smartcard detect ECM&EMM messages that are being replayed by an attacker.

SF_RIP Residual Information Protection

This security feature makes sure that keys are cleared from memory after their use.

FCS_CKM.4> Cryptographic keys are securely erased.
FDP_RIP.1> Public keys and secret keys are properly de-allocated.

6.6 Illegal Updating Code Protection

SF.CODE_UPDATE : Updated Code Authentication and Integrity

This security feature allows code updating by the operator.
It verifies the authentication signature and the code version before its activation and use. The code integrity is checked with a hash algorithm.

FDP_ACC.2/EMM&ECM> EMM are controlled before being imported.
FDP_DAU.1/EMM&ECM> Verification of the validity of EMM is performed to ensure correct integrity of data imported.
FDP_ITC.1/ECM&EMM> Verification of the validity of EMM is performed to ensure correct integrity when importing into the smartcard.
FIA_ATD.1/OPERATOR> Operator public key is used to verify integrity of EMM and EEPROM code.
FIA_UID.2/Operator> Only the operator can perform EEPROM code updates.
FMT_MOF.1> Only the operator is allowed to modify the behavior of the security functions.
FMT_MTD.1> Only the operator can perform EEPROM code updates.
FMT_SMR.1> Two roles are defined to allow correct EMM operations (which include EEPROM code updates).
FCS_CKM.3/AUTH> Access to a key is done to ensure FCS_COP.1 operation.
FCS_COP.1/AUTH> Cryptographic operations : a public/private key algorithm is used to authenticate EEPROM code.
FCS_COP.1/HASH> Cryptographic operations : a hash algorithm is used to hash EEPROM code.

SF.CODE_CTRL: Updated Code Control

This security feature controls code version before granting service access.

FMT_MOF.1> Only the operator is allowed to modify the behavior of the security functions.
FMT_SMF.1> EEPROM code can be updated by the operator.

6.7 Stored data protection

SF.DATA_INT: Data Integrity Detection

Secret keys are protected with a CRC and a reference.
Tracers are set up in memory to detect potential memory zones erasing.
Certain types of data are not associated to secrets and thus, are subject to security risks. They are protected by a redundancy mechanism.

FDP_SDI.2> Integrity control on User data.
FPT_TST.1> Integrity control on TSF data.

SF.DATA_CRYPT: Data Confidentiality Protection

Secret keys are ciphered with a specific symmetric algorithm with fixed-length key to ensure data protection.

FCS_CKM.3/STB_MESS> Access to a key is done to ensure FCS_COP.1 operation.
FCS_COP.1/STB_MESS> Cryptographic operations; encryption and decryption using a symmetrical algorithm are used to cipher keys stored in EEPROM.

6.8 Protection

SF.FAILURE-ERROR

This security feature detects hardware and software functioning faults, identify potential violations, and reacts to preserve a secure state.

FAU_SAA.1> TSF is able to monitor the events and to identify a potential violation.
FPT_FLS.1> TSF ensures a secure state is preserved when faults are detected.
FDP_SDI.2> Reaction on detection of integrity error on User data.
FIA_AFL.1> When an ECM or an EMM is not successfully authenticated, the smartcard rejects the message.

SF.SELF_TEST

This security feature ensures that the smartcard does startup tests to ensure integrity of security mechanisms of the TOE.

FPT_TST.1> Self tests ensure correct operation of the TOE.

SF.SIDE_CHANNEL-TAMPERING

This security feature uses hardware mechanisms to protect against DPA, SPA and Timing Attacks. It also uses software mechanisms to protect against DFA attacks.

FPT_PHP.3> Protection against exploitability of fault injection attacks.
FPR_UNO.1> Protection against DPA, SPA, Timing attacks.

7 PP claim

7.1 PP reference

The Security Target claims compliance to the PP9911.
The following section (§7.2) identifies the additions made to the PP9911, i.e. those required by the TOE specific features in terms of security. The last section (§7.3) outlines the few changes currently needed to adapt the PP to Common Criteria version 3.1.

7.2 PP additions

7.2.1 Additional assumption

There is an additional assumption to PP/9911 : A.STB (phase 7).

7.2.2 Additional threats

The following threats have been added to PP/9911 threats, from the specific nature of the Pay-TV application :

TOE specific threats (phase 7) :
T.RIGHT_MOD
T.KEY_DIS
T.AC_MOD
T.STB_ABUSE
T.RECORD_ABUSE
T.UPDATE_MOD
T.UPDATE_LOCK
T.REPLAY

7.2.3 Additional security objectives

The following security objectives for the TOE have been added to PP/9911 (they basically correspond to the additional threats listed in §7.2.2) :

O.DATA_WRITE
O.SECURE_ENTITLEMENT
O.STB_PAIRING
O.SECURE_RECORD
O.SECURE_UPDATE
O.UPDATE_VERSION
O.INDEX

An additional environment objective (arising from the additional assumption in §7.2.1) has been added :

OE.STB

7.2.4 Additional security functional requirements

Security functional requirements have been added to the claimed PP :
FDP_IFC.1 and FDP_IFC.1 (Control Word export policy)
FTP_ITC.1 (secure channel between STB and TOE)

7.2.5 Additional assurance requirements

There is no additional assurance requirement to the set identified in the PP (see however the adaptations to CCv3.1 in §7.3).

7.3 PP adaptations

Pending an official update of PP/9911 to Common Criteria version 3.1, the following features were adapted in the Security Target with the approval of the French Certification Body :

- Security Functional requirements : removal of FPT_SEP.1 (this SFR does not exist anymore in Part 2 of CC v3.1)
- Assurance Requirements : use of CCv3.1 EAl4 package. The changes versus the EAL4 CCv2.3 package are the following :
    - Use of ADV_IMP.1 (CCv3.1) instead of ADV_IMP.2 (CCv2.3)
    - Use of ATE_DPT.2 (CCv3.1) instead of ATE_DPT.1 (CCv2.3)

  The augmentations to EAL4 are ALC_DVS.2 and AVA_VAN.5 (deemed equivalent to ALC_DVS.2 and AVA_VLA.4 in CCv2.3). The Strength of Function (SOF) claim from CCv2.3 has also been deleted (this SOF concept is not used anymore in CCv3.1).

8 Rationale

This chapter presents the evidence that 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.

8.1 Security objectives rationale

8.1.1 Threats and security objectives

The following tables show which security objectives counter which threats phase by phase.

During phase 1, the Smart Card ES is developed and Application Data are specified for all other phases.

The TOE is a functional product designed during phase 1, considering that the only purpose of the Embedded Software is to control and protect the operation of the TOE during phases 4 to 7 (product usage). The global security requirements to consider in the TOE, during the development phase, are the security threats of the other phases. Such threats are identified in chapter 3 of this PP. This is why the PP addresses the functions used in phases 4 to 7 but developed during phase 1.

T.CLON*

> The TOE being constructed can be cloned, but also the construction tools and document can help clone it. During phase 1, Since the product does not exist, it cannot contribute to countering the threat. For the remaining phases 4 to 7, the TOE participates in countering the threats.

T.DIS_INFO*

> This threat addresses disclosure of sensitive information concerning security mechanisms implemented in the IC and/or in the ES and known by the software developer, in order to meet the overall security objectives of the TOE. Sensitive information are transmitted by the IC designer to the Smart Card Software developer during phase 1.

T.DIS_DEL*

> This threat addresses disclosure of software or Application Data which is delivered, from phase 1 to phase 2 for software embedding. As the data is not yet implemented in the TOE, the threat can only be countered by environmental procedures.

T.DIS_DEL1

> This threat addresses disclosure of software or data during delivery from phase 1 to phases 4 to 6. As the data is not yet implemented in the TOE, the threat can only be countered by environmental procedures.

T.DIS_DEL2

This threat addresses disclosure of software or data which is delivered from phase 1 to phases 4 to 6. As the data is not yet implemented in the TOE, the threat can only be countered by environmental procedures.

T.DIS_ES1

Although the ES is created in phase 1, it is active throughout the life of the Smart Card, and therefore this threat can be carried out during any and all of phases 1 through 7. During phases 1 and 2, as the product does not yet exist, so it cannot contribute to countering the threat.

T.DIS_TEST_ES

Tests concerning the embedded software or software to be embedded are carried out in phase 1. This threat is countered by environmental procedures, of which the tests themselves are part.

T.T_DEL*

This threat addresses the theft of software or Application Data which is delivered for software embedding, from phase 1 to phase 2. As the data is not yet implemented in the TOE, the threat can only be countered by environmental procedures.

T.T_TOOLS

TOE development tools are only used during phase 1, so this threat can exist only during phase 1. As the TOE does not yet exist, these threats are countered by environmental procedures.

T.T_SAMPLE2

TOE samples are used only during phase 1, so this threat can exist only during phase 1. The theft or unauthorized use of samples are countered by environmental procedures.

T.MOD_DEL*

This threat addresses modification of software or data which is delivered for software embedding, in phase 2.

T.MOD_DEL1

This threat addresses modification of Application Data during delivery to the IC packaging manufacturer, phase 4, the Finishing process manufacturer, phase 5, and for the Personalizer, phase 6.

T.MOD_DEL2

This threat addresses modification of Application Data which is delivered to the IC packaging manufacturer, phase 4, the Finishing process manufacturer, phase 5, and for the Personalizer, phase 6.

T.MOD

Modification of software and Application Data can be done during ES design in phase 1. Since the product does not exist, the threat can only be countered by environmental objectives.

T.MOD_SOFT*

Once developed, the ES and the Application Data can be modified during any of the phases 4 to 7.

T.DIS_ES2

Disclosure of ES and sensitive data can compromise security. During phases 4 to 7, the TOE must counter the unauthorized disclosure of the ES and the Application Data.

T.T_ES

This threat covers the unauthorized use of stolen cards during the different phases of the Smart Card life cycle as well as the misappropriation of rights of the Smart Cards.

T.T_CMD

This threat includes the diversion of the hardware or the software, or both, in order to execute non authorized operations.

T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE

The loading, execution and modification of programs shall not endanger the security of the TOE, especially to avoid interference between applications.

T.RIGHT_MOD

This threat addresses unauthorized modification or creation of customer rights into the TOE in phase 7.

T.KEY_DIS

This threat covers disclosure of keys during transfert with TOE in phase 7.

T.AC_MOD

This threat addresses unauthorized modification of entitlement control message in phase 7.

T.STB_ABUSE

This threat covers unauthorized use of TOE in phase 7 : use of TOE with non authorized STB.

T.RECORD_ABUSE

This threat covers another unauthorized use of TOE in phase 7 : use of TOE to access data recorded by another customer.

T.UPDATE_MOD

This threat covers unauthorized use, modification or creation of software update in phase 7.

T.UPDATE_LOCK

This threat covers unauthorized blocking of software update in phase 7.

T.REPLAY

This covers unauthorized use of obsolete message in phase 7.

8.1.2 Threats addressed by security objectives

8.1.2.1 Security objectives for the TOE

During phase 1, the TOE does not yet exist, so there is no threat on the TOE itself. For the phases 4 to 7, the following table indicates that each threat is mapped to at least one security objective during the life of the TOE:

Threats/Obj.	O.TAMPER_ES	O.OPERATE*	O.FLAW*	O.DIS_MECHANISM2	O.DIS_MEMORY	O.MOD_MEMORY	O.CLON*	O.DATA_WRITE	O.SECURE_EXCHANGE	O.SECURE_ENTITLEMENT	O.STB_PAIRING	O.SECURE_RECORD	O.SECURE_UPDATE	O.UPDATE_VERSION	O_INDEX
T.CLON*				X	X		X								
T.DIS_ES2	X	X	X	X	X					X					
T.T_ES	X	X	X			X									
T.T_CMD	X	X	X			X									
T.MOD_SOFT*	X	X	X			X									
T.KEY_DIS									X	X					
T.MOD_LOAD	X	X	X			X	X	X	X				X		
T.MOD_EXE	X	X	X			X	X	X	X				X		
T.MOD_SHARE	X	X	X			X	X	X	X				X		
T.RIGHT_MOD								X							
T.UPDATE_MOD								X					X	X	
T.UPDATE_LOCK													X	X	
T.STB_ABUSE									X		X				
T.RECORD_ABUSE									X		X	X			
T.AC_MOD										X					
T.REPLAY															X

Table 5: Mapping of security objectives for the TOE from phase 4 to 7

The TOE shall use state of the art technology to achieve the following IT security objectives; for that purpose, when Smart Card IC physical security features are used, the specification of these physical security features shall be respected :

O.TAMPER_ES

Addresses the protection of the security critical parts of the TOE and protects them from any disclosure, either directly by bypassing protections or indirectly by interpretation of physical or logical behavior. This feature addresses disclosure centered threat T.DIS_ES2.

Security mechanisms must especially prevent the unauthorized modification of security attributes and functional parameters such as the life cycle sequence flags. This feature addresses the modification oriented threats T.MOD_SHARE and T.MOD_SOFT*.

The ES must be designed to avoid interpretations of electrical signals from the hardware part of the TOE. These characteristics cover either the currents, voltages, power consumption, radiation, or timing of signals during the processing activity of the TOE.

The TOE has to provide physical and logical security mechanisms to avoid fraudulent access to any sensitive data, such as passwords, cryptographic keys or authentication data. This covers illegal use or duplication of TOE: T.T_ES, T.T_CMD, T.MOD_LOAD and T.MOD_EXE.

O.CLON*

Addresses the threat of cloning the TOE, T.CLON*. This objective limits the possibility to access any sensitive security relevant information of the TOE, and thus covers T.MOD_LOAD, T.MOD_EXE and T.MOD_SHARE.

O.OPERATE*

The TOE must ensure the correct continuation of operation of its security functions. Security mechanisms have to be implemented to avoid fraudulent usage of an interruption or change in sequence in the normal process order to avoid thesecurity protection. These interruptions or changes may becarried out either by physical or by logical actions (statically or dynamically).

This objective covers the unauthorized change of security attributes managing the access to sensitive information which materialize T.DIS_ES2, T.MOD_SHARE and T._MOD_SOFT*, as well as actions of skipping internal protections of the TOE, which result in threats T.T_ES, T.T_CMD, T.MOD_LOAD and T.MOD_EXE.

O.FLAW* Addresses the threats T.DIS_ES2, T.T_ES, T.T_CMD, T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE and T.MOD_SOFT* by preventing any unauthorized modification of the TOE which could lead to malfunctions in security mechanisms during its design, production or operation.

O.DIS_MECHANISM2 The TOE shall ensure that the security mechanisms are protected against unauthorized disclosure, to combat the threats T.DIS_ES2 and T.CLON*.
The security mechanism can use either the hardware or the software or both. Such mechanisms must be kept confidential, especially the way to use them in order to counter threats.

O.DIS_MEMORY* The TOE shall ensure that sensitive information stored in memories is protected against unauthorized access. Such disclosure realizes the threats T.DIS_ES2, and can lead to T.CLON*.
This is obvious for secret information, but also applies to access controlled information.

O.MOD_MEMORY* The TOE shall ensure that sensitive information stored in memories is protected against any corruption or unauthorized modification, which covers T.MOD_SOFT* and modification by unauthorized loading which covers T.MOD_LOAD.
The TOE shall also ensure that any loss of integrity cannot endanger the security, especially in case of modification of system flags or security attributes. It helps to combat T.MOD_EXE and T.MOD_SHARE threats.
The TOE shall prevent the fraudulent modification of such information as indicators or flags in order to go backwards, through the card life cycle sequence to gain access to prohibited information. Such modifications are a first step to realize T.T_ES or T.T_CMD.

O.DATA_WRITE The TOE shall limit data write access to confidential and authenticated EMM (Entitlement Management Message) of the operator. It helps to prevent T.MOD_EXE, T.MOD_LOAD, T.MOD_SHARE especially when smartcard software update occurs with management audience EMM. It also helps to prevent modification of customers rights and unauthorized software update: T.RIGHT_MOD, T.UPDATE_MOD.

O.SECURE_EXCHANGE The TOE shall use secure protocol and procedures between the card and the terminal. It helps to prevent T.KEY_DIS, T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE. It also contribute to protect against STB-related abuses such as T.STB_ABUSE and T_RECORD_ABUSE.

O.SECURE_ENTITLEMENT The TOE shall use to manage ECM (Entitlement Control Message) data secure protocols for confidentiality and authentication. It helps to cover T.DIS_ES2, T.KEY_DIS, T.AC-MOD.

O.STB_PAIRING STB and TOE shall be paired before use. This objective protects against STB specific abuses : T.RECORD_ABUSE and T.STB _ABUSE.

O.SECURE_RECORD The TOE used secure protocol to protect the data write on external media. It prevents T.RECORD_ABUSE.

O.SECURE_UPDATE The TOE shall not permit loading or executing of unauthorized Update Software. It protects against T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE, T.UPDATE_MOD and T_UPDATE_LOCK.

O.UPDATE_VERSION The TOE shall control Software update versioning. It protects against T.UPDATE_MOD and T.UPDATE_LOCK.

O_INDEX The TOE shall control message sequence. It prevents T.REPLAY.

8.1.2.2 Threats and security objectives for the environment

The following figure maps the security objectives for the environment relative to the various threats, during phase 1:

Threats/Obj.	OE.DEV_TOOLS*	OE.DEV_DIS_ES	OE.SOFT_DLV*	OE.INIT_ACS	OE.SAMPLE_ACS
T.CLON*	X	X	X	X	X
T.DIS_INFO*		X			
T.DIS_DEL*	X	X	X	X	
T.DIS_ES1	X	X		X	
T.DIS_TEST_ES	X	X	X		
T.T_DEL*			X		
T.T_TOOLS	X				
T.T_SAMPLE2					X
T.MOD_DEL*		X	X	X	
T.MOD		X		X	

Table 6: Mapping of security objectives for the environment from phase 1

OE.DEV.TOOLS* The development tools shall provide for the integrity, availability and reliability of both programs and data. This specificity will protect against cloning, T.CLON*.
Information Technology equipment are used to develop, to test, debug, modify, load the ES and personalize the TOE. Therefore, these equipment shall be accessible only by authorized personnel. This is to cover threats based on illegal access to equipment or development information: T.DIS_ES1,T.DIS_TEST_ES, T.T_TOOLS.

OE.DEV_DIS_ES The ES shall be designed in a secure manner, in order to focus on the integrity availability and confidentiality of programs and data. It must be ensured that confidential information (such as user manuals and general information on defined assets) are only delivered to the parties authorized personnel. This covers the disclosure based threats: T.DIS_INFO*, T.DIS_DEL*, T.DIS_ES1 and T.DIS_TEST_ES, and thus helps to combat T.MOD, T.MOD_DEL* and T.CLON*.

OE.SOFT_DLV* O.SOFT_DLV addresses all the threats applicable to the delivery of the Smart Card Embedded Software to the IC designer since it requires the application of a trusted delivery and verification procedure (T.T_DEL*) maintaining the integrity (T.MOD_DEL* , T.MOD) and the confidentiality of the software if applicable (T.DIS_DEL*). and of initialization data (T.DIS_ES1) and test information (T.DIS_TEST_ES). This contributes to combat the threat T.CLON*.

OE.INIT_ACS It must be ensured that Initialization Data are only delivered to the parties authorized personnel and that Initialization Data integrity is achieved. This covers disclosure based threats: T.DIS_DEL* and T.DIS_ES1. It also covers the theft based threats: illegal modification T.MOD_DEL* and T.MOD. All of this contributes to combat T.CLON*.

OE.SAMPLE_ACS Samples used to run tests shall be accessible only by authorized personnel in order to avoid illicit use of such samples. These sample must be considered as sensitive parts, especially because they can be used (with the relevant parameters) in the place of trusted TOEs. This covers T.T_SAMPLE2 and T.CLON*.

The following figure maps the security objectives for the environment relative to the various threats on delivery, during phases 4 to 6:

Threats/Obj.	OE.DLV_DATA	OE.TEST_OPERATE*
T.DIS_DEL1	X	
T.DIS_DEL2		X
T.MOD_DEL1	X	
T.MOD_DEL2		X

Table 7: Mapping of security objectives for the environment to threats on delivery for phase 1 to phase 4 to 6

OE.DLV_DATA Protects against disclosure or modification of Application Data during the delivery to other manufacturers, and thus covers T.DIS_DEL1 and, T.MOD_DEL1.

OE .TEST_OPERATE Protects against disclosure or modification of Application Data delivered to other manufacturers and thus covers T.DIS_DEL2 and T.MOD_DEL2.

8.1.2.3 Assumptions and security objectives for the environment

This section demonstrates that the combination of the security objectives is suitable to satisfy the identified assumptions for the environment. Each of the assumptions for the environment is addressed by objectives.

The following table outlines the objectives which contribute to the satisfaction of the assumptions. For clarity, the table does not identify indirect dependencies.

Phases		Phase 1					Delivery process for phases 4 to 7			Phases 4 to 6		Phase 7			
	Assumptions	OE.DEV_TOOLS	OE.DEV_DIS_ES	OE.SOFT_DLV*	OE.INIT_ACS	OE.SAMPLE_ACS	OE.DLV_PROTECT*	OE.DLV_AUDIT*	OE.DLV_RESP*	OE.TEST_OPERATE	OE.SECURE_PERSO	OE.USE_DIAG*	OE.STB	OE.USE_ORG	OE.USE_RENEWAL
1	A.DEV_ORG*	X	X	X											
4 to 7	A_DLV_PROTECT*						X								
4 to 7	A.DLV_AUDIT*							X							
4 to 7	A.DLV_RESP*								X						
4 to 6	A.USE_TEST*									X					
4 to 6	A.USE_PROD*									X					
4 to 6	A.SECURE_PERSO										X				
7	A.USE_DIAG*											X			
7	A.STB												X		
7	A.USE_ORG													X	
7	A.USE_RENEWAL														X

Table 8: Mapping to assumptions of objectives for the environment

With respect to the set of environment objectives from the PP, OE.SECURE_PERSO, OE.STB, OE.USE_ORG and OE.USE_RENEWAL are the additional environment objectives covering the additional assumptions (A.STB, A.USE_ORG and A.USE_RENEWAL) :

OE.SECURE_PERSO The personalization operations in phases 4 to 6 must be performed along procedures that shall ensure that people dealing with the personalization operations have got the required skill, training, knowledge and tools to meet securely the personalization requirements defined by the embedded software developer. This security objective instantiates the assumption A.SECURE_PERSO.

OE.STB

The descrambling control words must be unciphered only in the pay TV flow descrambling circuit. Those CW must not be in clear into the STB. Pairing and confidentiality keys located into the STB must be protected for confidentiality and integrity. This security objective instantiates the assumption A.STB.

OE.USE_ORG

Only authorized personnel have access to tools in charge of EMM and ECM secure message generation. Secure message generators use specific crypto smartcards to generate management and exploitation messages. Specific cryptosmartcards must be accessible only to authorized personnel. This security objective instantiates the assumption A.USE_ORG.

OE.USE_RENEWAL

Access rights to the TV service must be renewed regularly for security reasons at least monthly). Ciphering key (CWs) must change each 10 seconds approximately. This security objective instantiates the assumption A.USE_RENEWAL.

These additions complement elements from the PP : they do not introduce any inconsistency.

8.2 Security requirements rationale

This section demonstrates that the combination of the security requirements objectives is suitable to satisfy the identified security objectives.

8.2.1 Security functional requirements

The following table demonstrates which security functional requirements contribute to the satisfaction of each TOE security objective. For clarity, the table does not identify indirect dependencies.

Security Requirements	O.TAMPER_ES	O.OPERATE*	O.DIS_MECHANISM2	O.DIS_MEMORY*	O.MOD_MEMORY*	O.FLAW*	O.CLON*	O.DATA_WRITE	O.SECURE_EXCHANGE	O.SECURE_ENTITLEMENT	O.STB_PAIRING	O.SECURE_RECORD	O.SECURE_UPDATE	O.UPDATE_VERSION	O.INDEX
EAL4 requirements						X									
FAU_SAA.1	X	P	P	X	X	X	P								
FCS_CKM.3/ECM_EMM	X	P		P	P		P	X		X			X		
FCS_CKM.3/STB_MESS	X	P		P	P		P		X		X	X			
FCS_CKM.3/AUTH	X	P		P	P		P	X		X			X		
FCS_CKM.4	X	P		P	P		X	X					X	X	
FCS_COP.1/ECM_EMM	X			X			P	X		X			X		
FCS_COP.1/STB_MESS	X			X			P		X		X	X			
FCS_COP.1/AUTH	X			X			P	X		X			X		
FCS_COP.1/HASH	X			P	P			X	X	X	X	X	X		
FDP_ACC.2/EMM&ECM	X	P	X	X	P		P	X		X			X		
FDP_ACF.1/EMM&ECM	X	P	X	X	P		P	X		X			X		
FDP_DAU.1/EMM&ECM	X	P			X		P	X		X			X		
FDP_ETC.1/CW export				X	P				X						
FDP_IFC.1/CW export									X			X			
FDP_IFF.1/CW export									X			X			
FDP_ITC.1/EMM&ECM				X				X		X	X		X		
FDP_RIP.1	X			P									X		
FDP.SDI.2		P			X										
FIA_AFL.1	X	P			P		P	X		X					
FIA_ATD.1/OPERATOR	X	P			P			X		X			X		
FIA_ATD.1/STB	X	P			P				X		X	X			
FIA_UAU.1/STB	X			X	X		P		X			X			

(to be continued next page)

FIA_UAU.2/OPERATOR	X			X	X		P	X		X			X		
FIA_UAU.3/OPERATOR	X			X	X		P	X		X					
FIA_UAU.4	X			X	X		P	X					X		
FIA_UID.1/STB	X			X	X		P		X			X			
FIA_UID.2/OPERATOR	X			X	X		P	X		X			X		
FIA_USB.1	X			X	X		P		X		X	X			
FMT_MOF.1	X	X	X	P	P		P						X		
FMT_MSA.1	X	P	X	P	P		P	X		X					
FMT_MSA.2	X	P	X	P	P		P	X							
FMT_MSA.3	X	P	X	P	P		P	X							
FMT_MTD.1				X	X		P	X					X		
FMT_SMF.1													X		
FMT_SMR.1	X	X						X			X		X		
FPR_UNO.1	X	P		X	X		X								
FPT_FLS.1	X													X	X
FPT_PHP3	X	X	X	X	X		X		X						
FPT_TDC.1	X				X										
FPT_TST.1		P			X										
FTP_ITC.1				P			P		X		P				

Table 9: Mapping of security functional requirements and objectives

Legend : P :Partial ; X :relevant

This section describes why the security functional requirements are suitable to meet each of the TOE security objectives.

The assurance requirements contribute to the satisfaction of the O.FLAW* security objectives. They are suitable because they provide the assurance that the TOE is designed, implemented and operates so that the IT security requirements are correctly provided.

As the TOE is able to detect potential physical violation via sensors and related circuitry, and logical violation through TSF enforcing functions, FAU_SAA.1 meets the security objectives O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY* and partially O.OPERATE* and O.DIS_MECHANISM2 in order to monitor events and indicate a potential violation of the TSP.

Cryptographic support functional requirements FCS_CKM.3/ECM_EMM supports the access control to the assets such as ECM by key management in the case of illicit access, or any attempt to steal sensitive information. These functions combine to meet the security objectives of O.TAMPER_ES, O.DATA_WRITE, O_SECURE_ENTITLEMENT, O_SECURE_UPDATE and participate in meeting O.OPERATE*, O.DIS_MEMORY*, O.MOD_MEMORY*, and O.CLON* requirements.

Cryptographic support functional requirements FCS_CKM.3/STB_MESS supports the access control to the assets such as control words by key management in the case of illicit access, or any attempt to steal sensitive information. These functions combine to meet the security objectives of O.TAMPER_ES, O.SECURE_EXCHANGE, O_STB_PAIRING, O_SECURE_RECORD and participate in meeting O.OPERATE*, O.DIS_MEMORY*, O.MOD_MEMORY*, and O.CLON* requirements.

Cryptographic support functional requirements FCS_CKM.3/AUTH supports the access control to the assets such as ECM and EMM messages by key management in the case of illicit access, or any attempt to steal sensitive information. These functions combine to meet the security objectives of O.TAMPER_ES, O.DATA_WRITE, O_SECURE_ENTITLEMENT, O_SECURE_UPDATE and participate in meeting O.OPERATE*, O.DIS_MEMORY*, O.MOD_MEMORY*, and O.CLON* requirements.

Cryptographic support functional requirements FCS_CKM.4 supports the access control to the assets by key destruction in the case of illicit access. These functions combine to meet the security objectives of O.TAMPER_ES, O_CLON*, O.DATA_WRITE, O.SECURE_UPDATE, O.UPDATE_VERSION and participate in meeting O.OPERATE*, O.DIS_MEMORY* and O.MOD_MEMORY* requirements.

FCS_COP.1/ECM_EMM which supports data encryption controls the assets such as ECMs and EMMs by encryption. This function combines to meet the security objectives of O.TAMPER_ES, O.DIS_MEMORY*, O.CLON*, O.DATA_WRITE, O.SECURE_ENTITLEMENT, O.SECURE_UPDATE.

FCS_COP.1/STB_MESS which supports data encryption controls the assets such as ECMs, EMMs APDU and CW by encryption. This function combines to meet the security objectives of O.TAMPER_ES, O.DIS_MEMORY*, O.CLON*, O.SECURE_EXCHANGE, O.STB_PAIRING, O.SECURE_RECORD.

FCS_COP.1/AUTH which supports data signature controls the assets such as ECMs and EMMs by authentication. This function combines to meet the security objectives of O.TAMPER_ES, O.DIS_MEMORY*, O.CLON*, O.DATA_WRITE, O.SECURE_ENTITLEMENT, O.SECURE_UPDATE.

FCS_COP.1/HASH which supports data integrity controls the assets such as messages by hashing. This function combines to meet the security objectives of O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY, O.DATA_WRITE, O.SECURE_EXCHANGE, O.SECURE_ENTITLEMENT, O.STB_PAIRING, O.SECURE_RECORD, O.SECURE_UPDATE.

Access control functional requirements, FDP_ACC.2/EMM&ECM and FDP_ACF.1/EMM&ECM control the access conditions. This fulfills the security objectives, O.TAMPER_ES, O.DIS_MECHANISM2, O.DIS_MEMORY*, O.DATA_WRITE, O.SECURE_ENTITLEMENT, O.SECURE_UPDATE and partially O.OPERATE*, O.MOD_MEMORY*, O.INDEX and O.CLON*.

The Data authentication functional requirement FDP.DAU.1/EMM&ECM assures the objectives O.TAMPER_ES, O.MOD_MEMORY*, O.DATA_WRITE, O.SECURE_ENTITLEMENT and O.SECURE_UPDATE. It contributes to the correct operation of TOE, O.OPERATE, and O .CLON*.

The export to outside TSF control functions FDP_ETC.1/CW export contributes to realization of O.DIS_MEMORY* and O.SECURE_EXCHANGE. They contribute to the correct operation of the TOE, O.MOD_MEMORY*.

The information flow control functions FDP_IFC.1/CW export and FDP_IFF.1/CW export contributes to realisation of O.SECURE_EXCHANGE and O.SECURE_RECORD.

Sensitive information can be securely imported from outside in order to be processed or stored inside the TOE. The TSF control functions FDP_ITC.1/EMM&ECM, contribute to the realization of O.DIS_MEMORY*, O.DATA_WRITE, O_SECURE_ENTITLEMENT, O.STB_PAIRING and O.SECURE_UPDATE.

FDP_RIP.1 prevents access to residual sensitive information which was temporarily stored in memories during previous states of processing. This functional requirement meets O.TAMPER_ES, O.SECURE_UPDATE objectives and partially O.DIS_MEMORY*.

The FDP_SDI.2 functional requirement meets O.MOD_MEMORY* objective. It also contributes to the correct operation of TOE which covers O.OPERATE*.

Identification and authentication functional requirements FIA_AFL.1 and FIA_ATD.1/OPERATOR which manage illicit OPERATOR authentication attempts and related security attributes meet O.TAMPER_ES, O.DATA_WRITE, O.SECURE_ENTITLEMENT, objectives and partially O.OPERATE*,O.MOD MEMORY*. FIA_AFL1 also contributes to the correct operation of the TOE, O.CLON*. FIA_ATD.1/OPERATOR also enhance secure update of the TOE, O.SECURE_UPDATE.

Identification and authentication functional requirement FIA_ATD.1/STB manages illicit STB authentication attempts and related security attributes meet O.TAMPER_ES, O.SECURE_EXCHANGE, O.STB_PAIRING, O.SECURE_RECORD objectives and partially O.OPERATE*,O.MOD MEMORY*.

Identification and authentication functional requirement FIA_UAU.1/STB allows access to public information stored in memory from an external access such as a terminal. On the other hand, FIA_UAU.2/OPERATOR requires successful operator authentication before any TSF action. They contribute to security objectives O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY*, and O.SECURE_EXCHANGE, O.SECURE_RECORD for FIA_UAU.1/STB, and O.DATA_WRITE, O.SECURE_ENTITLEMENT, O.SECURE_UPDATE for FIA_UAU.2/OPERATOR. They also partially contribute to the correct operation of the TOE, O.CLON*.

Identification and authentication functional requirements FIA_UAU.3/OPERATOR prevents and detects unauthorized access to stored memory for an authenticated OPERATOR and thus contributes to security objectives O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY*, O.DATA_WRITE, O.SECURE_ENTITLEMENT It also partially contributes to the correct operation of the TOE, O.CLON*.

Identification and authentication functional requirement FIA_UAU.4 enhances single use authentication mechanism for ECMs and EMMs and contributes to security objectives O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY*, O.DATA_WRITE, and O.SECURE_UPDATE. It also partially contributes to the correct operation of the TOE, O.CLON*.

Timing of identification functional requirement FIA_UID.1/STB allow a set of restrictive actions before user authentication is successful and contributes to security objectives O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY*, O_SECURE_EXCHANGE, O_SECURE RECORD and contributes partially to O.CLON* objective.

Timing of identification functional requirement FIA_UID.2/OPERATOR allow action only after operator authentication is successfully done and contributes to security objectives O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY*, O.DATA_WRITE, O.SECURE_ENTITLEMENT, O.SECURE_UPDATE and contributes partially to O.CLON* objective.

User subject binding requirement FIA_USB.1 enhances rules regarding user security attributes and contributes to security objectives O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY*, O_SECURE_EXCHANGE, O.STB_PAIRING, O.SECURE_RECORD and contribute partially to O.CLON* objective.

FMT_MOF.1 restricts the ability to modify the access conditions or the user rights. This functional requirement meets O.TAMPER_ES, O.OPERATE*, O.DIS_MECHANISM2, O.SECURE_UPDATE and partially O.DIS_MEMORY*, O.MOD_MEMORY*, O.CLON* objectives.

Management of TSF data functional requirements FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3 which control the usage, modification and deletion of the security attributes meet the O.TAMPER_ES, O.DIS_MECHANISM2, O.DATA_WRITE objectives and contribute to the correct operation of the TOE, O.OPERATE*, O.DIS_MEMORY*, O.MOD_MEMORY and O.CLON*. FMT_MSA.1 contributes to O.SECURE_ENTITLEMENT objective.

The FMT_MTD.1 functional requirement controls the authorization to access or modify sensitive information. This functional requirement meets O.DIS_MEMORY*, O.MOD_MEMORY*, O.DATA_WRITE, O_SECURE_UPDATE objectives and partially O.CLON*.

The FMT_SMF.1 functional requirement allows definition of specific management function of the TOE. This requirement meets the O.SECURE_UPDATE objective.

FMT_SMR.1 functional requirement allow the definition of security roles for the TSF and meets the O.TAMPER_ES, O.OPERATE*, O.DATA_WRITE, O.STB_PAIRING, and O.SECURE_UPDATE objectives.

The FPR_UNO.1 functional requirement meets O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY*, and O.CLON* especially to protect against the observation of internal processes of the TOE. It provides protection against unauthorized disclosure of sensitive information during operation of the TOE under control of the Embedded Software. Thus, it also contributes to O.OPERATE* security objective.

The FPT_FLS.1 functional requirement protects TSF from failure and allows definition of a secure state, thus it meets O.TAMPER_ES, O.UPDATE_VERSION, and O.INDEX objectives.

FPT_PHP.3 (Resistance to physical attack) functional requirement meets O.TAMPER_ES, O.DIS_MEMORY*, O.MOD_MEMORY* and O.CLON*. FPT_PHP.3 also meets O.OPERATE*, O.DIS_MECHANISM2 and O.SECURE_EXCHANGE. It should be noted that FPT_PHP.1 (Passive detection of physical attack) is not relevant for Smart Cards because it is always more secure not to give information on the origin of physical attacks to the outside world, since this could help an attacker to counter a security mechanism.

The FPT_TDC.1 functional requirement meets O.MOD_MEMORY* and O.TAMPER_ES objectives. The TOE shall interpret consistently the information coming from trusted IT products.

FPT_TST .1 functional requirement meets O.MOD_MEMORY* and partially O.OPERATE*. The suite of self tests may run only during initial start-up of the TOE, aiming at the integrity of executable code and/or sensitive memory content. Each test yields a global answer depending of the result of the test. This test has to be defined, but it is clear that a correct authentication process or a correct cryptographic operation demonstrate the correct operation of the TSF during execution of commands.

FTP_ITC.1 functional requirement meets O.SECURE_EXCHANGE and partially O.DIS_MEMORY*, O_CLON and O_STB_PAIRING objectives. This functional requirement is selected for the TOE and for its IT environment (i.e. the STB).

8.2.2 Security functional requirements dependencies

This section demonstrates that the dependencies between components of security functional requirements are satisfied (excepted for FAU_GEN.1 that a smartcard cannot implement, as argued in PP/9911).

SFR dependencies are presented in the following table :

Requirements	CC-required dependencies	Dependencies satisfaction
FAU_SAA.1	FAU_GEN.1	The dependency of FAU_SAA.1 with FAU_GEN.1 is not applicable to the TOE. The FAU_GEN.1 component forces many security relevant events to be recorded (due to dependencies with other functional security components) and this is not achievable in a Smart Card since many of these events result in card being in an insecure state where recording of the event itself could cause a security breach. It is then assumed that the function FAU_SAA.1 may still be used to notify potential violations without these specific events being audited.
FCS_CKM.3/ECM/EMM	FDP_ITC.1, FCS_CKM.4	OK
FCS_CKM.3/STB_MESS	FDP_ITC.1, FCS_CKM.4	OK
FCS_CKM.3/AUTH	FDP_ITC.1, FCS_CKM.4	OK
FCS_CKM.4	FDP_ITC.1	OK
FCS_COP.1/ECM_EMM	FDP_ITC.1, FCS_CKM.4	OK
FCS_COP.1/STB_MESS	FDP_ITC.1, FCS_CKM.4	OK
FCS_COP.1/AUTH	FDP_ITC.1, FCS_CKM.4	OK
FCS_COP.1/HASH	FDP_ITC.1, FCS_CKM.4	OK
FDP_ACC.2/EMM&ECM	FDP_ACF.1	OK
FDP_ACF.1/EMM&ECM	FDP_ACC.1, FMT_MSA.3	OK (chosen FDP_ACC.2 is hierarchically superior to required FDP_ACC.1)
FDP_DAU.1/EMM&ECM	-	OK
FDP_ETC.1/CW export	FDP_IFC.1	OK
FDP_ITC.1/CW EXPORT	FDP_IFC.1	OK
FDP_IFC.1/CW EXPORT	FDP_IFF.1	OK
FDP_IFF.1/CW EXPORT	FDP_IFC.1, FMT_MSA.3	OK
FDP_ITC.1/ECM&EMM	FDP_ACC.2, FMT_MSA.3	OK
FDP_RIP.1	-	OK
FDP_SDI.2	-	OK
FIA_AFL.1	FIA_UAU.2	OK (chosen FIA_UAU.2/OPERATOR is hierarchically superior to required FIA_UAU.1)
FIA_ATD.1/OPERATOR	-	OK
FIA_ATD.1/STB	-	OK
FIA_UAU.1/STB	FIA_UID.1	OK
FIA_UAU.2/OPERATOR	FIA_UID.2	OK
FIA_UAU.3/OPERATOR	-	OK
FIA_UAU.4	-	OK
FIA_UID.1/STB	-	OK
FIA_UID.2/OPERATOR	-	OK
FIA_USB.1	FIA_ATD.1	OK (FIA_ATD.1/STB)
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	OK
FMT_MSA.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1	OK (chosen FDP_ACC.2 is hierarchically superior to required FDP_ACC.1)
FMT_MSA.2	FDP_ACC.1, FMT_MSA.1, FMT_SMR.1	OK (chosen FDP_ACC.2 is hierarchically superior to required FDP_ACC.1)
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	OK
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	OK
FMT_SMF.1	-	OK

(to be continued next page)

Requirements	CC-required dependencies	Dependencies satisfaction
FMT_SMR.1	FIA_UID.1	OK (FIA_UID.1/STB, FIA_UID.2/OPERATOR)
FPR_UNO.1	-	OK
FPT_FLS.1	-	OK
FPT_PHP.3	-	OK
FPT_TDC.1	-	OK
FPT_TST.1	-	OK
FTP_ITC.1	-	OK

Table 10: SFR dependencies

8.2.3 Security assurance Requirements

An assurance level of EAL4 was chosen for this TOE, since it is intended to defend against sophisticated attacks. The assurance level was chosen to meet the assurance expectations of digital signature, encryption/decryption applications in a DVB-T television standard smartcard access control scheme.

Additional assurance requirements to the well defined EAL4 package are required due to the definition of the TOE (see below).

8.2.3.1 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. This assurance component is a higher hierarchical component to EAL4 (only ALC_DVS.1 is found in EAL4). Due to the nature of the TOE, there is a need to justify the sufficiency of these procedures to protect the confidentiality and the integrity of the TOE.
ALC_DVS.2 has no dependencies.

8.2.3.2 AVA_VAN.5 Advanced methodical vulnerability analysis

Due to the definition of the TOE, it must be shown to be highly resistant to penetration attacks. This is due to the fact that a Smart Card can be placed in a hostile environment, such as electronic laboratories.

This assurance requirement is achieved by the AVA_VAN.5 component. Independent vulnerability analysis is based on highly detailed technical information. The attacker is assumed to be thoroughly familiar with the specific implementation of the TOE. The attacker is presumed to have a high level of technical sophistication.