Vitale 2
on
ID-One Cosmo X²

Public Security Target

Issue : 3

DOCUMENT REVISION HISTORY			
Issue	**Date (dd/mm/yyyy)**	**Author**	**Purpose**
1	06/05/2026	IN Smart Identity	Initial version
2	12/05/2026	IN Smart Identity	§3.2, §3.4, §7.3.2, §7.3.3.1, §7.3.3.2, §9.2 updated
3	06/07/2026	IN Smart Identity	- §1.3, §1.4 and §1.5 updated - AES 192 bits removed - FCS_COP.1/GP_MAC: CBC replaced with CMAC - §2.1: OS developer name updated - §4.3: title added for each threat - Index table updated

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

1. Vitale Security Target

1.1 Product presentation

The Carte Vitale is a personal smart card issued by the GIE SESAM VITALE to all beneficiaries of the general scheme. It enables secure identification of the insured and the automation of health data exchanges with healthcare professionals and health insurance organizations. The product to be evaluated is a JavaCard applet embedded on a certified JavaCard platform, which itself runs on a certified IC, along with its associated security mechanisms.
The card is used in a constrained environment, particularly within healthcare information systems (doctor's office, pharmacy, hospital), to ensure the presentation of the insured, the transmission of electronic treatment forms (FSE), and where applicable, authentication in healthcare teleservices. By integrating strong authentication, access management, and sensitive data protection mechanisms, it directly contributes to protecting the privacy of insured people in the processing of their health data.
The functional scope of the TOE includes:

- The implemented cryptographic functions enable;
- The authentication of various stakeholders;
- Data sealing;
  - Management of access rights to certain sensitive embedded data;
- Secure communication with authorized terminals and readers;
- Mechanisms for access control and secure software updates.

The product is based on a separately certified Java Card platform and IC, meeting the Common Criteria requirements and the protection profile for JavaCard platforms (PP Java Card Open Configuration [PP_JAVACARD]) and for IC's ([PP0084]). The "Carte Vitale" business applet is installed and customized during an industrial pre-customization phase, followed by an activation phase controlled by health insurance organizations.
The product Common Criteria assessment aims to guarantee a high assurance level (EAL4+), with proven protection mechanisms against logical and physical attacks.
Thus, the Vitale Card is a secure and interoperable system, adapted to the challenges of health data protection in France, and can serve as a reference for digital health identity systems in a broader context.

1.2 ST Introduction

This document is the Security Target for the VITALE product on ID-One Cosmo X^2 platform which is an IN Smart Identity (aka INSI) specific Java Card implementation [JC] of the SESAM VITALE specification [FSP].
VITALE is the support of health services as defined in the SESAM VITALE context to offer government e-services.
The TOE addressed by the current ST is not based on a PP.
VITALE is a set of Java Card services intended to be used exclusively on ID-One Cosmo X^2 Java Card Platform, which is certified according to underlaying platform level indicated in [ST-PL]. This Platform is based on a StarChip Controller including IC Dedicated Software, which is itself certified according underlaying IC level indicated in [ST-IC] or [CR-IC].
This Security Target describes :

- The Target of Evaluation (TOE)
- The assets to be protected, the threats (T) to be countered by the TOE itself during the usage of the TOE,
- The organizational security policies (P), and the assumptions (A),
- The security objectives (OT) for the TOE and its environment (OE),
- The security functional requirements (SFR) for the TOE and its IT environment,
- The TOE security assurance requirements (SAR),
- The TOE Summary specification (TSS).

The assurance level for the TOE is CC EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ALC_FLR.3.

1.3 ST Reference

Title	Vitale 2 on ID-One Cosmo X^2 - Public Security Target
Reference	FQR 151007-556
Version	Ed 3
ITSEF	SERMA
Certification Body	ANSSI
Author	IN Smart Identity
CC Version	CC:2022
Assurance Level	EAL4 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.3
Protection Profiles	No PP claimed

1.4 TOE Reference

Developer	IN Smart Identity
TOE commercial name	Vitale 2 on ID-One Cosmo X^2
TOE version number	1

Applet name	Vitale 2 on ID-One Cosmo X^2
Applet version	3.0.4

JavaCard Platform name	ID-One Cosmo X^2 ; see [ST-PL]
JavaCard Platform version (SAAAAR code)	09A111
Platform Certificate	NSCIB-CC-2400104-01

IC Identifiers	See [ST-IC]
IC Ref. Certificate	See [CR-IC]

1.5 TOE Documentation

The TOE Guidance are AGD_OPE and AGD_PRE as listed in the two first lines of the following table. The other lines concern the application specification.

TOE GUIDANCE	
[AGD_OPE]	FQR 151007-239 Ed2 - AGD_OPE - Vitale2 Applet on Cosmo X2 - Manuel utilisateur
[AGD_PRE]	FQR 151007-238 Ed2- AGD_PRE - Vitale2 Applet on Cosmo X2 - Manuel de Pré-Personnalisation - Personnalisation
TOE SPECIFICATION	
[FSP]	FQR151007-236 Ed2– Specifications techniques

1.6 TOE Overview

The TOE is an integrated circuit chip embedding

- An Operating system providing:
  - Java Card interfaces, as specified in [JC]
  - Extended interfaces for targeted applications needs
- VITALE application compliant with [FSP]

The TOE is an application based on Java Card that is intended to be used in the SESAM VITALE system as well as for electronic signature application. It is designed to be fully compliant with [DIR]. It provides services containing data needed for generating electronic signatures on behalf of the Card Holder as well as for user authentication and specific functions that have been also considered during the evaluation, particularly in the vulnerabilities analysis AVA_VAN.5.
The TOE comprises:

- VITALE applications,
- The ID-One Cosmo X^2 Java Card platform [ST-PL],
- The StarChip Secure Smart Card Controller including IC Dedicated Software [ST-IC],
- The associated guidance documentation [AGD_OPE] and [AGD_PRE].

The following Figure describes the architecture of the card and highlights the components of the card that are part of the TOE.

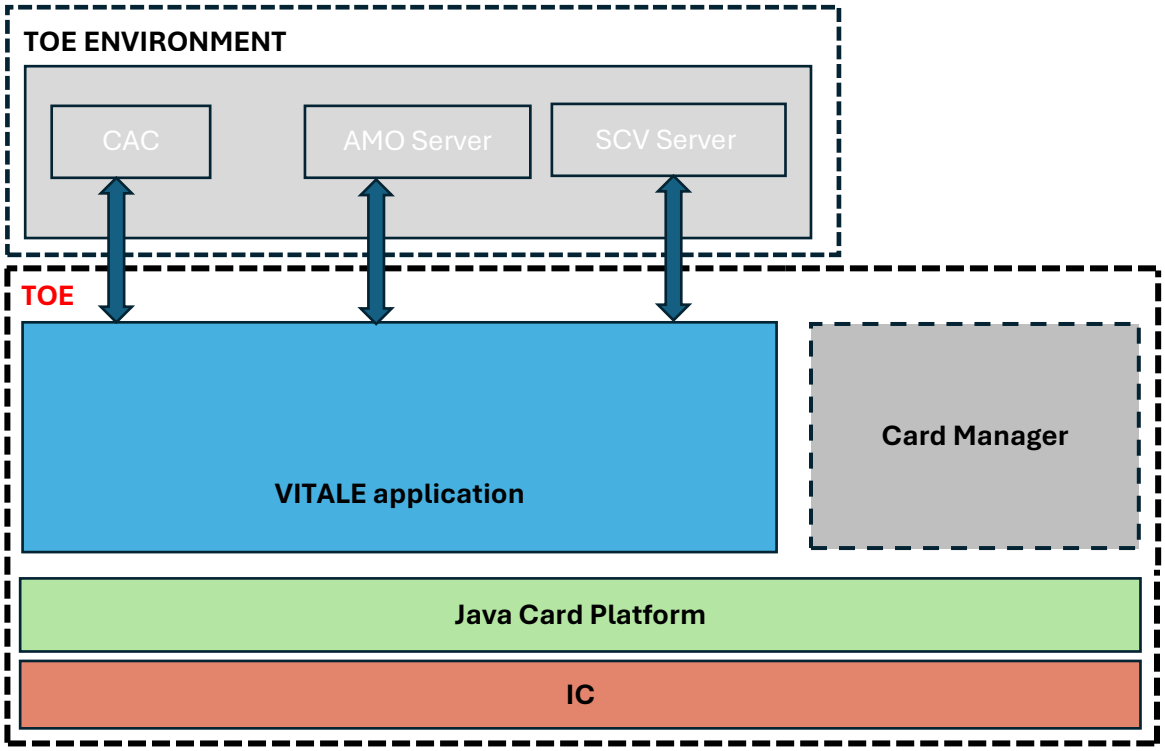

FIGURE 1: TOE PHYSICAL SCOPE

1.7 TOE Description

This section provides an overview of the components of the Sesame Vitale card.

1.7.1 Integrated Circuit

The IC is a StarChip dual interface component that supports ISO/IEC 14443 Type A [ISO14443] and ISO [ISO7816-4].
However, Vitale card is a "contact-only" smartcard compliant with [ISO7816] and supporting T=0 communication protocol only.
It is a hardware device composed of a processing unit, memory, security components and I/O interfaces. It has to implement security features able to ensure:

- The confidentiality and the integrity of information processed and flowing through the device,
- The resistance of the security IC to external attacks such as physical tampering, environmental stress or any other attacks that could compromise the sensitive assets stored or flowing through it.

More information on the chip is given in the related certification report [CR-IC] and related Security Target [ST-IC].

1.7.2 Java Card Platform ID-One Cosmo X²

The ID-One Cosmo X² Platform layer is responsible for:

- Providing an interface to all Applications that ensures that the Runtime Environment security mechanisms cannot be bypassed, deactivated, corrupted or otherwise circumvented;
- Performing secure memory management to ensure that:
  - Each Application's code and data (including transient session data) as well as the Runtime Environment itself and its data (including transient session data) is protected from unauthorized access from within the card. The Runtime Environment provides isolation between Security Domains via an Application Firewall.
  - When more than one logical channel is supported, each concurrently selected Application's code and data (including transient session data) as well as the Runtime Environment itself and its data (including transient session data) is protected from unauthorized access from within the card; The previous contents of the memory is not accessible when that memory is reused;
  - The memory recovery process is secure and consistent in case of a loss of power or withdrawal of the card from the card reader while an operation is in progress;
- Providing communication services with off-card entities that ensures the proper transmission (according to the specific communication protocol rules) of unaltered command and response messages
- Providing applications with cryptographic means to protect their communications.

More information on the ID-One Cosmo X² Platform is given in the related certification report [CR-PL] and related Security Target [ST-PL].

1.7.3 Sesam Vitale Card

The Vitale card is an application with VITALE specific functions. The complete set of commands used conforms to [FSP]. This includes the creation of the file system, the management of the DO and SDOs and the signature/seal keys, the cryptographic operations and the user authentication. The access to the services depends on the user access rights, SV card status and application status that perform the service. See § 1.10 Major security features of the TOE for more details about the services provided by SV.
The Vitale card includes the following specific functions:

- Seal calculation

This function enables data sealing with two keys, based on the algorithm TDES and AES.

- Protection mode modification

Three protection modes are defined. These modes define the access rules to the Sesam Vitale files and objects.

1.7.3.1 Vitale card Data

All data objects (DFs, EF and ADF) and DO/SDO are described in [FSP].
The set of data defined in the Vitale card are:

- Directories and Files (see [CARTE-NT-010] § 2.1)
- SDOs (see [CARTE-NT-010] § 2.3.1)
- Security Environment (SE) (see [CARTE-NT-010] § 2.3.2)

The set of data represented by cryptographic keys security environments SE associated services such as seal/signature, authentication mechanisms, etc. (see chapter 3.6 for more information).

1.7.4 Required non-TOE hardware/software/firmware

The TOE requires several external components not included within the TOE. These components are outside scope of the evaluation but are essential for the TOE's correct and secure operation. These non-TOE components are listed below:

- Smart Card Reader: ISO/IEC 7816-compliant contact reader.
- Terminal (CAC): Healthcare professional workstation
- Middleware Software: Middleware interfacing between the Vitale card and the CAC.
- Healthcare Information System: System used by health professionals to authenticate, query or update data related to the cardholder.

All non-TOE components listed above are assumed to operate correctly and securely within their intended functions. It is assumed that these components are configured in accordance with the applicable security policies and are not compromised.

1.8 TOE Functions

The TOE is a combination of hardware and software configured to securely create, use and manage:

1. symmetric signature creation data (*MAC Generation for seal creation*),
2. off-line asymmetric authentication,
3. on-line symmetric authentication,
4. symmetric mutual authentication and
5. secure messaging.

as main functionalities, and others security services.
All the keys (related to these functions or not) used by the TOE are protected during its whole life cycle.

1.9 Operational Environment

This section presents a functional overview of the TOE in its distinct operational environments:

1. The preparation environment interacts with the TOE to personalize it with the initial values of the reference authentication data (Manufacturer keys, pre-personalization key, personalisation key).
2. The signing environment where it interacts with a signer through a seal creation to sign data after authenticating the "signer" as its signatory. The seal creation application provides the data to be signed (DTBS) as input to the TOE seal creation function and obtains the resulting digital signature (MAC). Optionally, the TOE and the CAC may communicate through a trusted channel to ensure the confidentiality and the integrity of the DTBS.

3. The management environments where it interacts with the user or the CAC to perform management operations. A single device, e.g. a smart card terminal, may provide the required secure environment for management and signing.

1.10 Major security features of the TOE

The TOE provides TOE security features described in following chapters.

1.10.1 Symmetric Signature AMO and AMC (TDES/AES)

This feature performs a signature using dedicated TDES and AES keys (AMO Keys) for sealing data of the FSE.
Sesam Vitale organization Invoice signing:

- FSE with AMO key
- DRE with AMC key

– TLSi AMO: Signature of SAML Vitale tokens with AMO key
– EspacePro Access: Online authentication of the Vitale card

1.10.2 Authentication mechanisms

This feature provides different authentication mechanisms.

The following ones are the supported authentication in Vitale card:

- Internal Authentication
  - Symmetric or Online Authentication
  - Asymmetric or Offline Authentication
- Mutual Authentication
  - Symmetric

1.10.2.1 Symmetric Mutual authentication (AES)

This feature performs a Mutual Authentication process that is necessary for the CAC portal to access the Vitale card and then to set up Secure Messaging.

The Vitale card can be updated by the Administrator through the CAC portal. The Administrator can update the Vitale1 EF and invalidate the Vitale card.

The following requirements are performed online during the Mutual Authentication process:

- Use key based on symmetric AES algorithm;
- Use key provided by the GIE-SV organization;
- Use the challenge/response principle; and,
- Able to generate session keys that will be used for Secure Messaging.

This mechanism enables mutual authentication to be implemented between the card and a terminal to generate a set of session keys used to secure their communication via the secure messaging mechanism, see details in [FSP] § 3.9.3 and [IAS-PREMIUM] §8.2.2.

1.10.2.2 "Off-line" Asymmetric authentication (RSA+ ECC)

This feature is an Offline asymmetric authentication of the Vitale card using the *Short CVC certificate* (Asymmetric Internal Authentication, cf. [FSP] § 5.2.4.2.2).
This feature is used for:

- Cardholder authentication upon card reading
- Performed by the reader terminal

The supported algorithms and key sizes are:

- RSA 2048 and
- EC 256, 512, 521

1.10.2.3 "On-line" Symmetric authentication (TDES/AES)

Symmetric Authentication is used on terminals or on healthcare professional workstations. Prior to reading the data of the insured person, it is used to authenticate the Vitale card upon insertion to check if it has been issued by a genuine entity.
Symmetric internal authentication is done online by the server. The Vitale 2 card encrypts a challenge, provided by the server, and calculates the cryptogram of the result. The server checks the cryptogram and then decrypts and verifies the challenge. See section 7.2.2 of [FSP]

1.10.3 Secure Messaging (TDES/AES)

Mutual authentication between the Vitale card and the CAC portal makes it possible to negotiate a set of session keys to secure the application and card channel through the secure messaging mechanism.

The protected writing and updating of the Vitale card data is done online, and is based on either:

- the "secure messaging in integrity" alone; or,
- the "secure messaging in confidentiality and integrity", for certain sensitive data.

The "secure messaging in confidentiality" alone is **not** implemented.

The session keys established are global to the Vitale card.

A secure messaging session requires that all exchanges (commands) to be relayed in secure messaging, except for application selection handled by the underlying platform. See [FSP] §8 for more details.

1.10.4 Access Control

This feature manages the access to objects (files, directories, data, Keys, SE, DOs, SDOs, ...) stored in SV file system. It ensures secure management of secrets such as cryptographic keys. Access control is enforced by the APDU methods as specified in the interface defined in the functional specification [FSP]. This function ensures that it is not possible to bypass the access

controls. The access conditions are granted if the security conditions are fulfilled. Any access condition to fulfill is a combination of security conditions based on identified Keys/Secrets:

- Authentication of a remote administrator by symmetric or asymmetric mechanisms
- Communication protected in integrity and confidentiality

NB:

- GET DATA (CPLC and DF32, DF33) command do not require any Access Control to be performed. This service is always available, even in *Terminaison* state. Except for these cases, GET DATA is submitted to the access conditions as defined in [FSP].
- PUT DTA: the access conditions for this service are defined at during the DO/SDO creation.

1.10.5 Features from the Platform

This contains all security functionalities provided by the certified platform (JavaCard operation system):

- Protection against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.
- Protection against tampering and the stored assets cannot be retrieved or altered by physical manipulation
- Protection against physical attack and perform self-tests as described in [ST-PL].
- Security domains are supported by the Java Card platform.
- Cryptographic operations: Seal/Signature creation, secure messaging, Symmetric and Asymmetric Encryption/Decryption, Hash calculation, MAC and key exchange, etc.
- Patch mechanism, see guidance [JPATCH] in [ST-PL]: the underlying platform allows the loading of optional code and loading JavaCard applications:
    - Optional code can be loaded to upgrade the TOE (platform) at any time of product life cycle; this function is named JPatch.
    - Optional code (CodOp) can be loaded to upgrade an applet at any time of product life cycle.
    - Applications can be loaded on the flash memory, at pre-personalisation, personalisation or use phase. During post-issuance, the loading of other applets will be possible only under control of GIE Sesam Vitale organization.

2 TOE Life Cycle

The TOE life cycle is shown in the following Figure. It is described in terms of the following four life cycle phases.

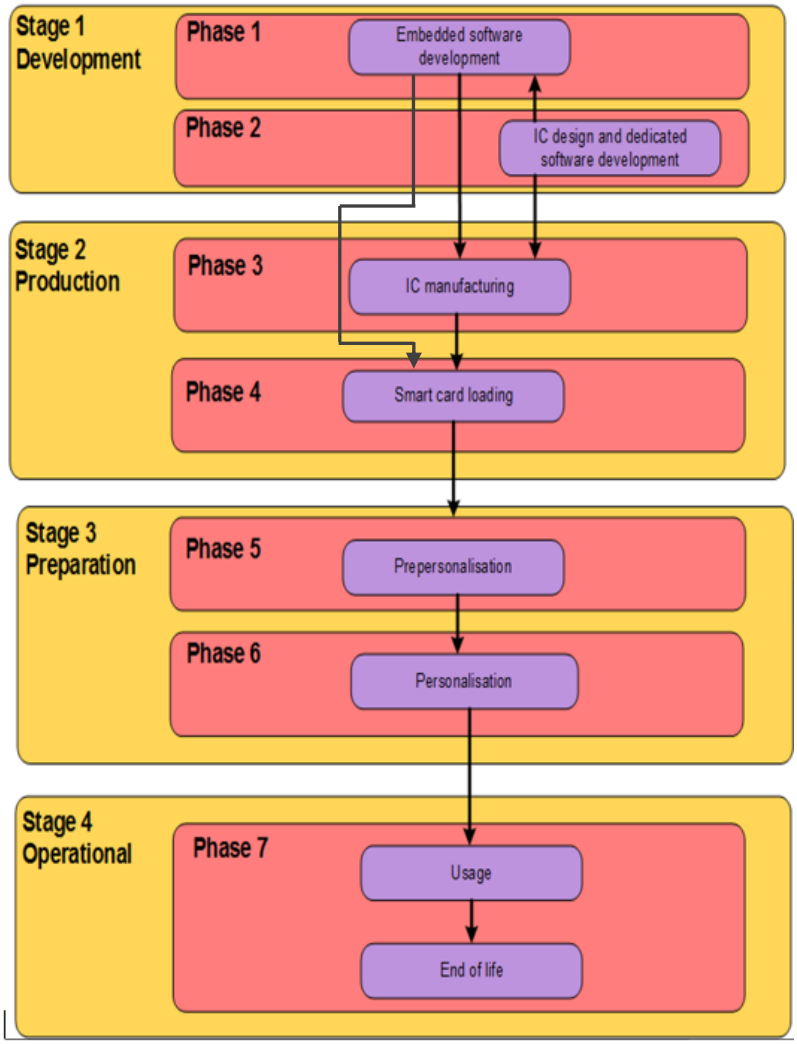

FIGURE 2 LIFE CYCLE OVERVIEW

2.1 Development Stage

The development environment encompasses the environment in which the TOE is developed, i.e.

- ID-One Cosmo X^2 Java Card Platform components
- Vitale card

This stage is composed of two phases:

- Phase 1: *Embedded software development*
- Phase 2: *IC design and dedicated software development*

The IC Developer (StarChip):

- Designs the IC, develops the IC dedicated software and provides information, software or tools to the Embedded software developer (INSI).
- Receives the Embedded software from the developer, through trusted delivery and verification procedures.
- Builds the database of the IC required to construct the photomask.

The Embedded Software Developer (IN Smart Identity) is in charge of:

- Specification, development and validation of the software VITALE application,
- Writing of the guidance documentation associated with these TOE components,
- Use of the guidance documentation for the IC.

Roles, Actors, Sites and coverage for this phase of the product life cycle are listed in the table below:

Phase	Role	Actor	Site	Covered by
1	VITALE Software Developer	INSI	Manila R&D site	ALC
1	ID-One Cosmo X^2 Java Card Platform	INSI	Refer to [CR-PL]	ALC
1	Redaction and Review of Documents	INSI	Manila and Courbevoie R&D sites	ALC
2	IC Developer	StarChip	Refer to [CR-IC]	ALC

2.2 Production Stage

This stage is composed of 2 phases with 3 options:

- Phase 3: *IC manufacturing*
- Phase 4: *Smart card loading*

The IC Manufacturer is responsible for producing the IC (manufacturing, testing, and initialization).
Also in phase 4, the Chip Provider (Foundry) key is imported in the TOE.
Depending on the intention, several life cycles are available, depending on when the Flash Code is loaded. The following tables present roles, actors, sites and coverage for this for this environment of the product life cycle and describe for each of them the TOE delivery point.

- **(Option 1)** the developer sends the image (containing both the Java Card platform and the VITALE application) to be flashed in the IC to the IC Manufacturer in *Phase 3*.

Role	Package to be loaded	Actor	Site	Covered by
IC Manufacturer	Image containing both Java Card platform and applet	IC Manufacturer	IC Manufacturer production plants [CR-IC]	ALC
TOE Delivery Point				

TABLE 1 IMAGE CONTAINING BOTH JAVA CARD PLATFORM AND VITALE APPLET IS LOADED AT IC MANUFACTURER (OPTION 1)

Or

- **(Option 2)** the platform developer sends the image (containing only the Java Card platform) to be flashed in the IC to the IC Manufacturer in *Phase 3*. Once the Java Card platform has been loaded, the package of VITALE application is securely delivered from the applet developer to the smart card loader. The CAP file of the applet is then loaded in the Java Card platform by the smart card loader as described in table below.

  TOE Delivery point:

  - In case CAP file is loaded in IN Smart Identity then TOE delivery is considered at the end of *Phase 4*,
  - Else TOE delivery is considered after *Phase 3*.

Role	Package to be loaded	Actor	Site	Covered by
IC Manufacturer	Image containing only Java Card Platform	IC Manufacturer	IC Manufacturer production plants (Refer to [CR-IC])	ALC
Smart card loader	CAP file of the Vitale applet	INSI	INSI audited sites (Haarlem, Ostrava)	ALC
		External Authorized Agent	Non-Audited INSI sites or External Sites	AGD

TABLE 2 CAP FILE OF VITALE APPLET IS LOADED THROUGH THE LOADER OF THE SMART CARD (OPTION 2)

Or

- **(Option 3)** the developer sends the image (containing both the JavaCard platform and the Vitale application) to be loaded in Flash (using the loader of the IC) to the smart card loader as described in table below.

  TOE Delivery point:

  - In case loading is done in IN Smart Identity then TOE delivery is considered at the end of *Phase 4*,
  - Else TOE delivery is considered after *Phase 3*.

Role	Package to be loaded	Actor	Site	Covered by
Smart card loader	Image containing both Java Card platform and Vitale applet	INSI	INSI audited sites (Haarlem, Ostrava)	ALC
		External Authorized Agent	Non-Audited INSI sites or External Sites	AGD

TABLE 3 IMAGE CONTAINING BOTH JAVA CARD PLATFORM AND VITALE APPLET IS LOADED THROUGH THE LOADER OF THE SMART CARD (OPTION 3)

The following table describes the physical delivery of the TOE components from ALC phase to

AGD phase:

TOE component	Form Factor of Delivery	Delivery method
Product: ID-One Cosmo X^2 embedding SV application	The package can be either of the following: - Chip modules contact-only embedded in ID1 cards, - Chip modules contact-only on reel	trusted courier
[AGD_PRE]	Electronic document	PGP-encrypted email
[AGD_OPE]	Electronic document	PGP-encrypted email
Key set	Electronic file	PGP encrypted parts on USB or CD media, off-line registered distribution by trusted courier.

2.3 Preparation Stage

This stage is composed of two Phases:

- Phase 5: *Smartcard Pre-personalization*
- Phase 6: *Smartcard Personalization*

The Pre-personalizer is responsible for:

- Vitale applet instance creation
- Initializing the Sesam Vitale File System (file structure),
- Loading in the Vitale application the Pre-personalization Data and the personalization keys.

The pre-personalized card is securely delivered from the Pre-personalizer to the Personalizer.

The Personalizer is responsible for:

a. Personalization:
   - The Personalizer authenticates him/herself to the TOE
   - The Personalizer imports the symmetric and asymmetric key necessary for Vitale card

b. Create the security policies to be applied to files and objects (access conditions for objects (DOs and SDOs) and files)

During these phases, the Vitale card is pre-personalized and personalized according to [AGD_PRE].

Card personalization is based on [EMV_CPS1.0] specifications.
Personalization security is based on a GP standard protocol SCP03.
Roles, Actors, Sites and coverage for this phase of the product life-cycle are listed in the table below:

Phase	Role	Actor	Site	Covered by
5	Pre-Personalizer	Pre-Personalization Agent off-card	The agent who pre-personalizes the Vitale Application for the holder (INSI sites or another agent)	[AGD_PRE]
6	Personalizer (Administrator)	Personalization Agent off-card	The agent who personalizes the SV application for the holder	[AGD_PRE]

2.4 Operational Stage

This stage is composed of two sub-parties:

- *Usage*
- *End Of Life*

Concerning the *Usage* part, the TOE is operational and used for the following functionalities:

1. Symmetric signature with key per use (Billing: FSE signature with AMO key / DRE with AMC key, SAML Vitale token signature for AMO TLSi)
2. "Offline" asymmetric authentication of the Vitale card (Using the Short CVC certificate)
3. "Online" symmetric authentication of the Vitale card (Used by the CAC portal prior to reading insured data)
4. Symmetric mutual authentication of the Vitale card (Used by the CAC portal to implement "Secure Messaging")
5. "Secure Messaging" (Used by the CAC portal to update insured data).

The *End Of Life* part is developed in [AGD_OPE]

Roles, Actors, Sites and coverage for this phase of the product life-cycle are listed in the table below:

Phase	Role	Actor	Site	Covered by
7	User or Administrator	User or Administrator	N/A	[AGD_OPE]

3 Conformance Claims

3.1 CC Conformance

This Security Target (ST) and the Target of Evaluation (TOE) claim conformance to the *Common Criteria for Information Technology Security Evaluation*, CC:2022, comprising:

Common Criteria	Conformance rationale
Part 1 [CC1]	Conformant
Part 2 [CC2]	Conformant
Part 3 [CC3]	Conformant
Part 5 [CC5]	Conformant
Errata [CC-ERRATA]	Conformant
[CEM]	Conformant

TABLE 1: CC CONFORMANCE RATIONALE

The Common Methodology for Information Technology Security Evaluation [CEM] has been considered.

3.2 Package Claim

This ST is conformant to the EAL4 package (Table 1) and composite product package (§6) as defined in [CC5].
The EAL4 have been augmented with the following requirement to fulfil the smartcard standard:

- ALC_DVS.2 (Sufficiency of security measures)
- AVA_VAN.5 (Advanced methodical vulnerability analysis)
- ALC_FLR.3 (Systematic flaw remediation)

3.3 PP Claim

This ST does not claim compliance with any Protection Profile.
However, this document is inspired by the SFR, SAR, OT.x OE.x from BAC PP [BAC PP] and [CC2] part 2 is used.
The underlying JavaCard Open Platform of the TOE is evaluated and certified in accordance with the Java Card™ System Protection Profile Open Configuration [PP_JAVACARD].
NB: During post-issuance, the loading of other applets will be possible only under control of GIE Sesam Vitale organization.

3.4 Conformance Rationale

The SFRs specified in this ST are the ones required by GIE SV.
The SARs are originally taken from SARs of CC:2022 part 3 [CC3] according to the package conformance EAL 4 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.3.

3.5 Conformance Statements

There is no conformance rationale with a protection profile, as there is no PP claim.

4 Security Problem Definition

4.1 Assets

Below are the assets of the TOE.

Personal Data:

File	Description
EF-PD	End user Identification Data
EF-Card	Dates
EF-PHOTO	End User photo
EF-GDO	Global Data Object
EF-DIR	Interoperability Information
EF-InfoTech	Technique Information
EF-Vitale 1	Fichier Vitale 1

Personalization Data (Perso_data)

Data that is written during the personalization phase:

- **Personal Data**
- SM Keys
- Administrator key set
- Vitale card authenticity key set
- Seal/Creation Key
- Authenticity of Vitale card data
- Key Usage Counter Limit
- Retry Counter Limit
- Insured's Rights

Pre-Personalization Agent keys (Pre-Perso_K)

This key set used for mutual authentication between the Pre-personalization agent and the chip, and secure communication establishment

Personalization Agent keys (Perso_K)

This key set used for mutual authentication between the Personalization agent and the Terminal/ chip, and secure communication establishment.

Pre-Personalization Data (Pre-Perso_Ident_data)

Data that is written during the pre-personalization phase:

- DGI DF48 (card type)
- DGI DF3F (physical serial number)

- CPLC update
- DEK (Data Encryption Key(s))
- Personalization Agent Key(s)

SM keys (SM_K)

This key set is used for secure communication establishment between the Terminal/CAC and the Vitale card.

Secure Messaging session keys (SM_Session_K)

Session keys are used to secure communication in confidentiality and authenticity.

GP session keys (GP_Session_K)

Session keys are used to secure communication in confidentiality and authenticity in GP transactions (during Pre-Perso and Perso phases).

Administrator key set (Admin_K)

This key set is used to authenticate the Administrators during Operation phase.

Vitale card authenticity key set (Card_Auth_K)

This key set is used to authenticate the Vitale card in online or off-line during Operation phase.

Data to be signed (DTBS)

Set of data which the user intends to sign/seal. Their integrity and unforgeability must be maintained.

Seal/Signature Creation Key (SC_K)

Symmetric Key used to perform a seal/signature operation. The confidentiality, integrity and Admin/User's sole control over the use of this key must be maintained.

Authenticity of the Vitale card data (Auth_Card_data)

The authenticity of the Vitale card personalized by the issuing organization (GIE Sesam Vitale) for the *Admin or User* to prove his possession of a genuine Vitale card.

Life-cycle State (LC_S)

The Life Cycle state related to the Pre-personalization, Personalization and USE phase of the application. The life-cycle of the application is modified by the different roles. Once a state is modified, it is not possible to come back to the previous state. This state determines the roles that can authenticate to the TOE and the actions they can perform.

4.2 Users/Subjects

S.Attacker

Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the TOE or to falsify the seal/signature. The attacker has got a high attack potential and knows no secret.

S.Admin

User in charge of performing the TOE initialization, TOE personalization or other TOE administrative functions. The S.Admin is acting as Admin for this user after successful authentication as “administrator”.

S.End Holder

The rightful holder of the Vitale card for whom the issuing organization (GIE Sesam Vitale) personalized the Vitale card.

S.Manufacturer

The Manufacturer is the default user of the TOE during *Phase 3* (see §2.2)

S.Pre-personalization Agent

This subject is responsible for the preparation of the Vitale card, i.e. creation of the MF and ADF and EFs and DO/SDOs. He also sets Personalization Agent keys.

S.Personalization Agent

The agent is acting on behalf of the issuing organization (GIE Sesam Vitale) to personalize the Vitale card *Admin* and *User* by some or all of the following activities

(i) establishing the identity the *holder* for personal data (name, birth date etc.) in the Vitale card,

(ii) Setting keys, DSs and SDOs, modifying the access condition to DO and EFs,

S.Terminal

A terminal is any technical system communicating with the TOE through the contact interface.

S.User

End user of the TOE who can be identified as administrator or end user. The subject S.User may act as Admin.

4.3 Threats

T.Transaction_Replay “Replay genuine transaction”

An attacker reissues multiple times a genuine transaction, potentially altering uncertified transaction data such as the healthcare professional's ID.

Threat agent: having high attack potential, being in possession of one or more legitimate Vitale card and in possession of Vitale reader system.

Asset: **SM_Session_K; Data to be signed ; Perso_data; Auth_Card_data**;

T.Counterfeit "Counterfeit of a genuine card"**:**

An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine Vitale card to be used as part of a counterfeit Vitale card. The attacker obtains information about the secrets used by a card for its authentication and signature mechanisms (i.e. cryptographic keys), then uses this information to emulate an authentic card.

This violates the authenticity of the Vitale card used for authentication of a user by possession of a Vitale card. The attacker may generate a new data set or extract completely or partially the data from a genuine Vitale card and copy them on another appropriate chip to imitate this genuine Vitale card.

The TOE provides protection by protecting the keys against disclosure and implementing processes and algorithms that avoid observing the results and processing.

Threat agent: having high attack potential, being in possession of one or more legitimate Vitale card.

Asset: **SM_K; SC_K**; **Pre-Perso_Ident_data**; **Perso_data; Admin_K; Card_Auth_K**

T.Abuse_Func "Abuse of functionality"**:**

An attacker may use functions of the TOE which shall not be used in the phase Operational in order :

1) To manipulate or to manipulate the user data
2) To manipulate (explore, bypass, deactivate or change) security features or functions of the TOE or
3) To disclose or to manipulate the TSF data.

This threat addresses the misuse of the functions for the initialization and personalisation in the operational phase after delivery to the Vitale card holder.

Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate Vitale card.

Asset: **LC_S, all**.

T.Usurpation_Insured_Rights "Usurpation rights" :

An attacker may manage to update the insured's rights.

Threat agent: having high attack potential, being in possession of a legitimate Vitale card.

Asset: **SM_K; SC_K; Insured's Rights (part of Perso_data)**

T.Sig/Seal_Forgery : “Forgery of the signature/seal”

An attacker forges a signed/sealed data object, maybe using a signature/seal which has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the user or admin or by third parties. The signature/seal created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

Threat agent: experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE

Asset: **SC_K**

T.SigF_Misuse : “Misuse of the seal creation function”

An attacker misuses the seal/signature creation function of the TOE to create SDO for data the Vitale card has not decided to sign.

Threat agent: having high attack potential with advanced knowledge of security principles and concepts employed by the TOE

Asset: **SC_K**

T.Forgery : "Forgery of data"

An attacker fraudulently alters all or part of the stored data, including its security data, to deceive the CAC (Vitale system). The attacker can also copy the entire Vitale card onto another card.

Threat agent: having enhanced basic attack potential, being in possession of one or more legitimate Vitale card.

Asset: **Perso_data;**

T.Information_Leakage : "Information Leakage"

An attacker may exploit information manipulated by the TOE during its use to disclose confidential data. Information leakage can be inherent to normal operation or caused by the attacker. Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or changes in processing times. This leakage may be interpreted as covert channel transmission, but it is more closely related to the measurement of operating parameters, which may be derived from contact interface measurements and can then be linked to the specific operation being performed. DEMA and DPA are examples. Additionally, the attacker may actively attempt to cause information leakage through fault injection (e.g., differential fault analysis).

Threat agent: having enhanced basic attack potential, being in possession of a legitimate Vitale card.

Asset: **SM_K; SM_Session_K; SC_K**; **Pre-Perso_K; Perso_K; GP_Session_K; Admin_K; Card_Auth_K**

T.Phys-Tamper : "Physical Tampering"

An attacker may perform physical probing of the Vitale card in order

(i) to disclose TSF Data or

(ii) to disclose/reconstruct the Embedded Software.

An attacker may physically modify the chip in order to

(i) modify security features or functions of the Vitale card,

(ii) modify security functions of the Embedded Software,

(iii) modify User Data or

(iv) to modify TSF data.

The physical tampering may be focused directly on the disclosure or manipulation of TOE User Data (e.g. user personal data) or TSF Data (e.g. authentication key of the Vitale card).

Physical tampering requires direct interaction with the chip internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, the hardware security mechanisms and layout characteristics need to be identified. Determination of software design including treatment of User Data and TSF Data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

Threat agent: having enhanced basic attack potential, being in possession of a legitimate Vitale card.

Asset: **Perso_data; SM_K, SM_Session_K, SC_K, Pre-Perso_K; Perso_K; GP_Session_K; Admin_K; Card_Auth_K**

T.Key_Usage “Key Access"

An attacker may use the internal secret keys of the TOE while the maximum of Key_Usage_Counter is reached.

The TOE protects the key usage through OT.Key_Usage_Counter “Configuration of Key Usage Counter” that support a Key Usage Counter that is decremented by one each time the key is used. Once the counter is depleted the key becomes unusable.

Threat agent: having high attack potential, being in possession of a legitimate Vitale card.

Asset: **SM_K; SC_K**.

T.ADMIN_Configuration “Tempering the TOE during administration”

An attacker may access the TOE at use phase (*Phase 7*) to try to:

(i) deactivate or modify security features or functions of the TOE or

(ii) circumvent, deactivate or modify security functions of the Vitale card.

Threat agent: having high attack potential, being in possession of one or more legitimate cards in Operational use phase.

Asset: **Auth_Card_data**

T.Preparation “Tampering the TOE during preparation”

An attacker may access TOE functions or modify sensitive information during the Pre-personalization and personalization phases.
Threat agent: having high potential and knowledge about Pre-personalization and Personalization phases.

Asset: **Pre-Perso_Ident_data, Perso_data**

4.4 Organisation Security Policy

Organizational security policy statements are made in terms of rules, practices or guidelines that must be followed by the TOE and its environment as established by the "GIE SV" scheme in which the TOE is to be used. The TOE is compliant with the organizational security policies that follow.

P.MANUFACT

The **Initialization Data** are written by the IC Manufacturer to identify the IC uniquely. The Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

P.PERSONALIZATION

"Personalization of the Vitale card by the issuing organization GIE Sesam Vitale only"

The issuing Organization, GIE Sesam Vitale, guarantees the correctness of the data with respect to the Vitale card end holder. The personalization of the Vitale card for the holder is performed by an agent authorized by the issuing Organization GIE Sesam Vitale only.

P.PERSONAL_DATA

The data stored on the chip (as for EFs DO/SDOs) are personal data of the end holder. These data groups are intended to be used only with agreement of the end holder by Terminals to which the Vitale card is presented. The Vitale card shall provide the possibility for the CAC to allow read access to these data only for terminals successfully authenticated based on knowledge of the Mutual Authentication Keys as defined in [FSP].

P.CRYPTO

Cryptographic functions used at Vitale functional specifications level (e.g. for Mutual Authentication or Vitale transactions) must be trusted to ensure the authenticity of transactions. Therefore, those cryptographic functions are expected to resist practical attacks. A practical attack is an attack that may occur during card lifespan or embedded key lifetime in the Vitale scheme, and that can be led by an organization and or an attacker with high expertise and computational resources. To that end: Vitale cryptographic functions shall be public and shall rely on mathematically sound cryptosystems according to the current state-of-the-art.

Secure parameters: Vitale cryptographic functions shall use security parameters (typically key lengths) strong enough to resist practical attacks.

Secure implementation: the implementation of Vitale cryptographic functions inside the TOE, including key storage, shall resist practical attacks.

The choice of the keys used for cryptographic operations shall comply with the [PG-083].

4.5 Assumptions

A.VITALE-Keys : "Cryptographic quality of Keys"

All keys being generated and imported must provide sufficient cryptographic strength and being compatible with [PG-083] recommendations. As a consequence of the [PG-083], it has to be ensured that these data provide sufficient entropy to withstand any attack.

A.SEC_PERSO : *"Protection during Pre-Personalization & Personalization"*

It is assumed that security procedures are used after delivery of the TOE up to *Phase 6* to maintain confidentiality and integrity of the TOE and of its data (to prevent any possible copy, modification, retention, theft or unauthorized use). This means that *Phase 5* and *Phase 6* after TOE Delivery are assumed to be protected appropriately.

Moreover, the Pre-personalization Agent and the Personalization Agent are responsible for ensuring the correctness of:

- the logical data with respect to the end user,
- the keys (symmetric and asymmetric),
- the contains of EF (EF.info for ex) DO/SDOs stored on the VITALE card.

5 Security Objectives

5.1 Security Objectives for the TOE

This section describes the security objectives for the TOE addressing the aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE.

OT.Card_Auth_Proof

"Proof of card authenticity"

The TOE must support the Terminal to verify the identity and authenticity of the card as issued by the identified issuing organization (GIE SV) by means of:

- Mutual Authentication as defined in [FSP] the Vitale card is genuine, and chip belong to each other as defined in [SV_DOC]. The Mutual Authentication process results in Secure Messaging session keys generation to guarantee the integrity and confidentiality of the exchanges.
- Internal Authentication as defined in [FSP] using a TOE internally stored confidential private key (RSA and EC).

OT.Preparation

"Protection of the TOE preparation"

During Pre-personalization and Personalization phases, the TOE must control the access to its sensitive information and its functions and must provide the means to secure exchanges using cryptographic functions. It must also ensure secure erasing of useless keys.

OT.ADMIN_Configuration

“Protection of the TOE administration”

In use phase (*Phase 7*), the TOE must ensure the administration actions are only authorized for Administrator. The TOE must control the access to its sensitive information and its functions and must provide the means to secure exchanges using cryptographic functions.

OT.Key_Usage_Counter

“Configuration of Key Usage Counter”

The TOE must protect the keys usage through OT.Key_Usage_Counter that supports a Key Usage Counter which should be decremented by one each time the key is used. Once the counter is depleted, the key should become unusable.

OT.AC_SM_Level

“Secure Messaging Level”

During Operational Use phase, the TOE must allow read access to sensitive data only if the Secure Messaging level reaches or exceeds the one specified in the Access Conditions data object.

OT.Data_Int

"Integrity of **Perso_data**"

The TOE must ensure the integrity of the ***Perso_data*** on the card against physical manipulation and unauthorized writing.

OT.Data_Conf

"Confidentiality of **Perso_data** "

The TOE must ensure the confidentiality of *the* ***Perso_data***. Read access to these objects is granted to *Terminal* successfully authenticated as Personalization Agent.

The TOE must ensure the confidentiality of the ***Perso_data*** during their transmission to the *Terminal*.

OT.Identification

"Identification and Authentication of the TOE"

The TOE must provide means to store product identification (IC and platform) and Pre-Personalization Data in its non-volatile memory (NVM).

IC and platform identification is managed by TOE platform. IC Identification Data unicity is ensured by TOE platform.

During *Phase 7*, the TOE shall identify itself only to a successful authenticated Terminal or Personalization Agent.

OT.Prot_Abuse-Func

"Protection against Abuse of Functionality"

After delivery of the TOE to the End holder, the TOE must prevent the abuse of test and support functions that may be maliciously used to

i. disclose critical User Data,

ii. manipulate critical User Data of the IC Embedded Software,

iii. manipulate Soft-coded IC Embedded Software or

iv. bypass, deactivate, change or explore security features or functions of the TOE.

Details of the relevant attack scenarios depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

OT.Prot_Inf_Leak

“Protection against Information Leakage”

The security objective OT.Prot_Inf_Leak requires the TOE to protect confidential TSF data stored and/or processed in the chip against disclosure by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines, which is addressed by the SFR FPT_EMS.1, by forcing a malfunction of the TOE, which is addressed by the SFR FPT_FLS.1 and FPT_TST.1, and/or by a physical manipulation of the TOE, which is addressed by the SFR FPT_PHP.3.

OT.Tamper_Resistance

“Tamper resistance”

The TOE shall prevent or resist physical tampering with specified system devices and components.

OT.Prot_Malfunction

"Protection against Malfunctions"

The TOE shall ensure its correct operation and the integrity of sensitive assets. In case of failure, the TOE shall be able to reach a secure state.

OT.Crypto

"Security of the crypto"

The TOE shall provide cryptographic algorithms at the state of the art and compatible with [PG-083] requirements. Keys generated by the TOE must have a sufficient level of entropy. Random number generators must also comply with [PG-083].

5.2 Security Objectives for the Operational Environment

The issuing organization (GIE SV) should implement the following security objectives of the TOE environment.
Appropriate 'Protection during Pre-Personalization & Personalization (OE.SEC_PERSO)' must be ensured after TOE Delivery up to the end of *Phase 6* as specified below.

OE.SEC_PERSO

"Protection during Pre-personalization & Personalization"

Phases after TOE Delivery up to the end of *Phase 6* must be protected appropriately to maintain confidentiality and integrity of the TOE and of its data (to prevent any possible copy, modification, retention, theft or unauthorized use).

Application Note:

The Pre-personalizer and the Personalizer have to use adequate measures to fulfil OE.SEC_PERSO for instance by using appropriate authentication mechanisms for pre-personalization and personalization functions during *Phase 5* and *Phase 6*.

OE.Auth_Key

"Auth Card Keys"

The card issuing organization (GIE SV) has to establish the necessary infrastructure in order to:

i. generate the Keys (for authentication, SM, on-line and off-line keys)
ii. ensure the secrecy of the Keys,
iii. store the Keys

5.3 Security Objectives Rational

5.3.1 Threats

T.Transaction_Replay addresses the threat an attacker may be able to re-read many times a genuine transaction and eventually modifies all or part of non-certified transaction data.

OT.ADMIN_Configuration ensures that access to sensitive data is only for authorized users and cryptographic functions ensure the secure exchanges.

OT.Key_Usage_Counter addresses the protection of keys usage and so limits an unlimited transaction replay.

OT.Data_Int and OT.Data_Conf are involved in guaranteeing the integrity and the confidentiality of the personal data and the transmission in secure way.

OT.AC_SM_Level restricts access to sensitive data based on Secure Messaging level, reducing risks of replay attacks.

T.Counterfeit

Deals with the possibility for an attacker to retrieve finally the secrets (seal/signature and/or authentication keys) so he can be able to imitate a genuine Vitale card.

OT.Card_Auth_Proof ensures the authenticity of the card through mutual authentication.

OT.ADMIN_Configuration ensures, in operational phase, that the TOE provides access to authorized administrators only.

OT.Prot_Inf_Leak provides protection against information leakage. The Vitale card is protected against disclosure of any information.

OT.Tamper_Resistance ensures the TOE is protected against physical tempering.

OE.SEC_PERSO ensures that the secrets are protected during Pre-personalization and Personalization phases. OE.Auth_Key ensures that the keys are intrinsically resistant.

T.Abuse_Func addresses attacks using functions not supposed to be executed in phase Operational in order to exploit TOE functions or data.

OT.Prot_Abuse-Func directly covers this threat by preventing misuse of embedded tests and support functions.

OE.SEC_PERSO changes the Life-cycle state and prevents return to a previous state and access to associated functions.

T.Usurpation_Insured_Rights deals with the possibility an attacker can modify the Vitale card parameters (insured rights).

OT.Preparation ensures that session keys are defined for Secure Messaging (GP and Vitale one) to secure exchanges during Pre-Personalization and Personalization phases and protect sensitive data.

OT.AC_SM_Level ensures that the sensitive data can be acceded only if the access conditions of the targeted objects are satisfied.

OE.SEC_PERSO ensures that the secrets are protected during Pre-personalization and Personalization phases.

T.Sig/Seal_Forgery addresses the threat of misuse of the TOE seal/signature creation function to create SDO by others than the “signatory” to create a seal/signature on data for which the “signatory” has not expressed the intent to sign.

OT.ADMIN_Configuration requires the TOE to restrict the access to sensitive information for only authenticated roles (administrators).

OT.Prot_Malfunction ensures the TOE is in an appropriate state and is operating correctly.

OT.Prot_Inf_Leak provides protection against information leakage. The Vitale card is protected against disclosure of any information.

T.SigF_Misuse deals with misusage of seal/signature creation function to sign data not decided by the Vitale card.

OT.ADMIN_Configuration requires the TOE to restrict the access to sensitive information for only authenticated roles (administrators).

OT.Data_Int is involved in guaranteeing the integrity of the personal data and the transmission in secure way.

OT.AC_SM_Level ensures that the sensitive data can be acceded only if the access conditions of the targeted objects are satisfied.

T.Forgery

OT.Data_Int protects the integrity of the stored data (personal data) and OT.Tamper_Resistance against physical tempering.

OT.Preparation requires the TOE to limit the writing access to the trustworthy Personalization Agent.

OT.Prot_Inf_Leak and OT.Data_Conf provide protection against information leakage. The Vitale card is protected against disclosure of any information.

OE.SEC_PERSO ensures that the secrets are protected during Pre-personalization and Personalization phases.

T.Information_Leakage

OT.Prot_Inf_Leak protects directly the TOE against information leakage.

OT.Data_Conf ensures confidentiality of personal data during storage and transmission, limiting leakage and misuse.

OE.SEC_PERSO ensures that the secrets are protected in confidentiality during Pre-personalization and Personalization phases.

T.Phys-Tamper

OT.Tamper_Resistance is directly addressed by this security objective against physical tempering.

OE.SEC_PERSO ensures that the secrets are protected in integrity during Pre-personalization and Personalization phases.

T.Key_Usage

OT.Key_Usage_Counter permits the TOE to protect the keys from unlimited usage.

OE.SEC_PERSO ensures that the counters are correctly initialized.

T.ADMIN_Configuration

OT.ADMIN_Configuration protects, in USE phase, from unauthorized access to TOE functions and from modifications of sensitive information exchanged between the TOE and the administration systems.

T.Preparation

OT.Preparation protects, in Pre-personalization and Personalization phases, from unauthorized access to TOE functions and from modifications of sensitive information exchanged between the TOE and the Personalization system.

OE.SEC_PERSO ensures that the secrets are protected during Pre-personalization and Personalization phases.

5.3.2 Organisational Security Policies

P.Manufact

The OSP P.Manufact “Manufacturing of the Vitale card” requires a unique identification of the IC by means of the Initialization Data and the writing of the Pre-personalization Data as being fulfilled by OT.Identification “Identification and Authentication of the TOE”.

P.Personalization

The OSP P.Personalization “Personalization of the Vitala card by issuing Organization GIE Sesam Vitale” addresses the:

i. loading of the logical data by the Personalization Agent as ensured in the security objective for the TOE environment OE.SEC_PERSO, and

ii. access control for the user data and TSF data as ensured by the security objective OT.Preparation "Protection of the TOE preparation". The security objective OT.Preparation "Protection of the TOE preparation" limits the management of TSF data and management of TSF to the Personalization Agent.

P.Personal_Data

The OSP P.Personal_Data “Personal data protection policy” requires the TOE

i. to support the protection of the confidentiality of the Vitale card by means of the CAC, once authenticated by OT.Card_Auth_Proof, and

ii. to enforce the access control for reading as decided by the issuing Organization GIE Sesam Vitale. This policy is implemented by the security objectives OT.Data_Int “Integrity of personal data” of the integrity of the stored data and during transmission and by the security objective OT.Data_Conf “Confidentiality of personal data” which ensures the protection of the confidentiality.

P.CRYPTO

This OSP requires that the cryptographic algorithms and keys used are robust and at the state of the art to resist attack.
OT.CRYPTO ensures that cryptography managed by the TOE is sufficiently robust.
OE.Auth_Keys ensures that keys generated outside of the TOE have a sufficient entropy.

5.3.3 Assumptions

A.VITALE-Keys

The assumption "Cryptographic quality of Keys" is directly covered by the security objective for the TOE environment OE.Auth_Key ensuring the sufficient key quality to be provided by the card issuing organization GIE Sesam Vitale.

A.SEC_PERSO

As OE.SEC_PERSO requires the Pre-personalization and the Personalization Agents to use adequate measures assumed in A.SEC_PERSO *"Protection during Pre-Personalization & Personalization"*, the assumption is covered by this objective.

5.3.4 SPD and Security Objectives

5.3.4.1 Threats and Objectives – Coverage

Threat	OT & OE
T.Sig/Seal_Forgery	OT.Prot_Inf_Leak; OT.ADMIN_Configuration; OT.Prot_Malfunction
T.SigF_Misuse	OT.ADMIN_Configuration; OT.Data_Int; OT.AC_SM_Level
T.Forgery	OT.Data_Int; OT.Tamper_Resistance; OT.Preparation; OT.Prot_Inf_Leak: OT.Data_Conf; OE.SEC_PERSO
T.Information_Leakage	OT.Prot_Inf_Leak; OT.Data_Conf; OE.SEC_PERSO

T.Phys-Tamper	OT.Tamper_Resistance; OE.SEC_PERSO
T.Transaction_Replay	OT.ADMIN_Configuration; OT.Key_Usage_Counter; OT.Data_Int; OT.Data_Conf; OT.AC_SM_Level;
T.Counterfeit	OT.Card_Auth_Proof; OT.ADMIN_Configuration; OT.Prot_Inf_Leak; OT.Tamper_Resistance; OE.SEC_PERSO, OE.Auth_Key
T.Key_Usage	OT.Key_Usage_Counter; OE.SEC_PERSO
T.ADMIN_Configuration	OT.ADMIN_Configuration
T.Abuse_Func	OT.Prot_Abuse-Func; OE.SEC_PERSO
T.Usurpation_Insured_Rights	OT.Preparation ; OT.AC_SM_Level; OE.SEC_PERSO
T.Preparation	OT.Preparation; OE.SEC_PERSO

5.3.4.2 OSP and objectives – Coverage

OSP	OT
P.MANUFACT	OT.Identification;
P.PERSONALIZATION	OT.Preparation; OE.SEC_PERSO
P.PERSONAL_DATA	OT.Data_Conf; OT.Card_Auth_Proof; OT.Data_Int
P.CRYPTO	OT.CRYPTO; OE.Auth_Keys

Table 4 OSPs and Security Objectives – Coverage

5.3.4.3 Assumptions and OE – Coverage

Assumption	OE
A.VITALE-Keys – Cryptographic quality of Keys	OE.Auth_Key
A.SEC_PERSO – Protection during Pre-Personalization & Personalization	OE.SEC_PERSO

Table 5 Assumptions and Security Objectives for the Operational Environment - Coverage

6 Extended Requirements

No extended requirement is defined in this Security Target.

7 Security Requirements

7.1 Security Functional Requirements (SFR)

This section describes the requirements imposed on the TOE in order to achieve the security objectives laid down in the previous chapter.

7.1.1 Class FCS Cryptographic Support

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a **hybrid deterministic** random number generator that implements: **CTR_DRGB as defined in NIST SP800-90**.
FCS_RNG.1.2 The TSF shall provide **numbers format 128-bits blocks** that meet **the average Shannon entropy per internal random exceeds 0.994**.

FCS_CKM.5/GP Cryptographic key derivation

FCS_CKM.5.1/GP The TSF shall derive cryptographic keys **GP Session Keys** from **KDF** in accordance with a specified cryptographic key derivation algorithm **[Algorithm]** and specified cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	key sizes	In TOE certified scope?	standard
AES	128 bits	Yes	[NIST SP 800-108]
	256 bits		

Application Note: This SFR generates the GP Session Keys.

FCS_COP.1/GP_ENC Cryptographic operation

FCS_COP.1.1/GP_ENC The TSF shall perform **secure messaging (GP) – encryption and decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	key sizes	In TOE certified scope?	standard
AES in CBC mode	128 bits	Yes	[FIPS_197]
	256 bits		

Application Note: This SFR uses GP Session Keys generated by FCS_COP.1/GP.

FCS_COP.1/GP_MAC Cryptographic operation

FCS_COP.1.1/GP_MAC The TSF shall perform **secure messaging – message authentication code** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	key sizes	In TOE certified scope?	standard
AES in CMAC mode	128 bits	Yes	[NIST_800_38B]
	256 bits		

Application Note: This SFR uses GP Session Keys generated by FCS_COP.1/GP.

FCS_COP.1/GP_AUTH Cryptographic operation

FCS_COP.1.1/GP_AUTH The TSF shall perform **symmetric authentication – encryption and decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	key sizes	In TOE certified scope?	standard
AES in CBC mode	128 bits	Yes	[FIPS_197]
	256 bits		

Application Note: This SFR uses Pre-Personalization Agent keys or Personalization Agent keys.

FCS_COP.1/GP_KEY_DEC Cryptographic operation

FCS_COP.1.1/GP_KEY_DEC The TSF shall perform **key decryption** in accordance with a specified cryptographic algorithm **[Algorithm]** and cryptographic key sizes **[Key Size(s)]** that meet the following: **[Standard]**

Algorithm	key sizes	In TOE certified scope?	standard
AES in CBC mode	128 bits	Yes	[FIPS_197]
	256 bits		

Application Note: This SFR uses DEK (Data Encryption Key) which is part of the Pre-Personalization data.

FCS_COP.1/Seal Cryptographic operation

FCS_COP.1.1/Seal

The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[cryptographic key sizes]** that meet the following: **[standard]**

cryptographic operation	cryptographic algorithm	cryptographic key sizes(bits)	In TOE certified scope?[1]	standard
Perform PSO COMPUTE CRYPTOGRAPHIC CHECKSUM on DATA	MAC 3DES	56	No	[ISO/IEC 9797-1]
		112		
		168	Yes	
	AES CMAC	128	Yes	[NIST_800_38B]
		256		

Application Note: This SFR uses Seal/Signature Creation Key.

[1] No' means this part is considered as legacy in **[PG-083]** but shall be mentioned as still used in the field

FCS_COP.1/Mutual-Auth Cryptographic operation

FCS_COP.1.1/Mutual-Auth

The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[cryptographic key sizes]** that meet the following: **[standard]**

cryptographic operation	cryptographic algorithm	cryptographic key sizes(bits)	In TOE certified scope?[2]	standard
Perform PSO COMPUTE CRYPTOGRAPHIC CHECKSUM on DATA	AES CBC	128	Yes	[NIST 800-38A]
		256		
	AES CMAC	128	Yes	[NIST_800_38B]
		256		

Application Note: This SFR uses Administrator key set.

FCS_COP.1/SM Cryptographic operation

FCS_COP.1.1/SM

The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[cryptographic key sizes]** that meet the following: **[standard]**

cryptographic operation	cryptographic algorithm	cryptographic key sizes (bits)	In TOE certified scope?	standard
Perform PSO COMPUTE CRYPTOGRAPHIC CHECKSUM on DATA	AES CMAC	128	Yes	[NIST_800_38B]
		256		

Application Note: This SFR uses Secure Messaging session keys generated by FCS_CKM.5/SM.

FCS_COP.1/Internal-Auth Cryptographic operation

FCS_COP.1.1/ Internal-Auth

The TSF shall perform **[cryptographic operation]** in accordance with a specified cryptographic algorithm **[cryptographic algorithm]** and cryptographic key sizes **[cryptographic key sizes]** that meet the following: **[standard]**

[2] No' means this part is considered as legacy in **[PG-083]** but shall be mentioned as still used in the field

cryptographic operation	cryptographic algorithm	cryptographic key sizes (bits)	In TOE certified scope?[3]	Standard
Perform PSO COMPUTE CRYPTOGRAPHIC "Internal Authentication" (on-line)	AES CBC AES CMAC	128	Yes	[NIST_800_38B]
		256		
Perform PSO COMPUTE CRYPTOGRAPHIC "Internal Authentication" (off-line)	RSASSA-PKCS1	2048	Yes	[RSA-PKCS#1][RSA-PKCS#1]
	RSASSA-PSS /SHA 256	2048		
	ECDSA with SHA256	256	Yes	[ECDSA]

Application Note: This SFR uses Vitale card authenticity key set.

FCS_CKM.5/SM Cryptographic Key Derivation

FCS_CKM.5.1/SM

The TSF shall derive cryptographic keys **SM Session Keys** from $K_{IFD/ICC}$ in accordance with a specified cryptographic key derivation algorithm **SHA-256** and specified cryptographic key sizes **AES-256** that meet the following **[NIST SP 800-108]**.

Application Note: This SFR uses SM keys.

FCS_CKM.3 Cryptographic Key Access

FCS_CKM.3.1

The TSF shall perform **cryptographic key access based on a usage counter** in accordance with a specified cryptographic key access method **"The key can be accessed as long as the counter does not reach the limit value"** that meets the following: **none**.

Application Note: All keys are associated with a usage counter. When this counter reaches the Key Usage Counter Limit, the key is no longer accessible.

FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.6.1

The TSF shall destroy **SM Session Keys (GP and Vitale session keys)** when **session is end or if an error occurs during SM exchanges.**

[3] No' means this part is considered as legacy in **[PG-083]** but shall be mentioned as still used in the field

FCS_CKM.6.2

The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method **clearKey()** that meets the following **Javacard API** [JCAPI].

7.1.2 Class FIA Identification and Authentication

FIA_UID.1 Timing of identification

FIA_UID.1.1

The TSF shall allow

(1) **to read the Initialization Data**

(2) to read CPLC data

(3) SELECT command

(4) GET DATA command

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_UAU.1 Timing of authentication

FIA_UAU.1.1

The TSF shall allow

(1) **to read the Initialization Data**

(2) to read CPLC data

(3) SELECT command

(4) GET DATA command

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.4 Single-use authentication mechanisms

FIA_UAU.4.1

The TSF shall prevent reuse of authentication data related to:

- **Mutual Authentication Mechanism**
- **GP authentication mechanism**
- **Symmetric Internal Authentication Mechanisms (online)**

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1
The TSF shall provide:

- **Mutual Authentication Mechanism**
- **GP authentication mechanism**

To support user authentication.
FIA_UAU.5.2
The TSF shall authenticate any user's claimed identity according to the **following rules:**

- **The TOE accepts the authentication attempt as Personalization Agent by GP authentication mechanism**
- **The TOE accepts the authentication attempt as Pre-Personalization Agent by GP authentication mechanism**
- **The TOE accepts the authentication attempt as Administrator by Mutual Authentication mechanism**

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1

The TSF shall detect when **an administrator configurable positive integer within 1 to 15 consecutive** unsuccessful authentication attempts occur related to **Mutual authentication Mechanism**.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **halt the process, return an error SW of '63 00' and block any new authentication attempt on this authentication key.**

Application Note:

The term "consecutive" has been added in this SFR to precise that consecutive unsuccessful authentication attempts are counted and that a successful authentication resets the counter to 0.

FIA_API.1 Authentication Proof of Identity

FIA_API.1.1
The TSF shall provide an **Internal Authentication and Off-line authentication** to prove the identity of the **Vitale card** by including the following properties **Possession of the Vitale card authenticity key set** to an external entity.

7.1.3 Class FPT Protection of the Security Functions

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1

The TSF shall ensure that the TOE does not emit emissions in excess over its attack surface in such amount that these emissions enable access to TSF data as specified in Table below.

ID	Emissions	Attack surface	TSF data	User data
1	power variations	Contact interface	- Pre-Personalization Agent Keys - Personalization Agent Keys - DEK (Data Encryption Keys) - SM Keys - Secure Messaging session keys - GP session keys - Administrator key set - Vitale card authenticity key set - Seal/signature generation Key	- Perso_data
2	timing variations			

FPT_TST.1 TSF testing

FPT_TST.1.1

The TSF shall run a suite of the following self-tests **at reset** to demonstrate the correct operation of **the TSF:**

(1) **Test of integrity of TSF data**

(2) **Test of integrity of TSF code**

FPT_TST.1.2

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

FPT_TST.1.3

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

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur:

1) **failure detected by TSF according to FPT_TST.1**
2) **tearing operations**
3) **power shortage**
4) **over and under voltage**
5) **over and under clock frequency**
6) **over and under temperature**
7) **integrity issues**

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1

The TSF shall resist **physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

7.1.4 Class FDP User Data Protection

FDP_ACC.1/Preparation Subset access control

FDP_ACC.1.1/Preparation

The TSF shall enforce the **Preparation SFP** on:

- **Subjects: the Pre-Personalization Agent, the Personalization Agent**
- **Objects:**
  - **Pre-Personalization Data (including Personalization Agent keys),**
  - **Personalization Data (Personal Data, SM Keys, Administrator key set, Vitale card authenticity key set, Seal/Creation Key, Authenticity of Vitale card data, Key Usage Counter Limit, Retry Counter Limit)**
  - **Life-cycle**
- **Operation: Writing, Reading**

FDP_ACF.1/Preparation Security attribute based access control

FDP_ACF.1.1/Preparation

The TSF shall enforce the **Preparation SFP** to objects based on the following:

- **Subjects: the Pre-Personalization Agent, the Personalization Agent**
- **Objects:**
  - **Pre-Personalization Data (including Personalization Agent keys),**
  - **Personalization Data (Personal Data, SM Keys, Administrator key set, Vitale card authenticity key set, Seal/Creation Key, Authenticity of Vitale card data, Key Usage Counter Limit, Retry Counter Limit)**
  - **Life-cycle**
- **Attribute: authentication status, life-cycle value**

FDP_ACF.1.2/Preparation

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

- **The Pre-Personalization Agent is allowed to write Pre-Personalization data and is allowed to read Pre-Personalization Data except secret keys when:**
  - **The Life-cycle value is Pre-Personalization.**
  - **The Pre-Personalization Agent is successfully authenticated.**
- **The Personalization Agent is allowed to write Personalization Data (Personal Data, SM Keys, Administrator key set, Vitale card authenticity key set, Seal/Creation Key, Authenticity of Vitale card data, Key Usage Counter Limit, Retry Counter Limit) and is allowed to read Personal Data when:**
  - **The Life-cycle value is Personalization.**
  - **The Personalization Agent is successfully authenticated.**

FDP_ACF.1.3/Preparation

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

FDP_ACF.1.4/Preparation

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **No role is allowed to read secret keys.**

FDP_ACC.1/Administration Subset access control

FDP_ACC.1.1/Administration

The TSF shall enforce the **Administration SFP** on:

- **Subject: Administrator**
- **Objects: Personal Data, DTBS, Life-Cycle**
- **Operation: Modifying, Reading, Creating seal**

FDP_ACF.1/Administration Security attribute based access control

FDP_ACF.1.1/Administration

The TSF shall enforce the **Preparation SFP** to objects based on the following:

- **Subject: Administrator with security attribute "Modify" and security attribute "Seal_creation"**
- **Object: Personal Data, DTBS, Life-cycle**

FDP_ACF.1.2/Administration

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

- **Administrator is allowed to read Personal Data when the following conditions are fulfilled:**
  - **The Life-cycle value is Operational.**
  - **The Administrator is authenticated.**
- **Administrator is allowed to create seal for DTBS with AES Key when the following conditions are fulfilled:**
  - **The Life-cycle value is Operational.**
  - **The Administrator has the access rights to generate a seal (Administrator.Seal_creation = True),**
  - **The Administrator is authenticated.**
- **Administrator is allowed to modify End User Personal Data when the following conditions are fulfilled:**
  - **The Life-cycle value is Operational.**
  - **The Administrator has the access rights to modify Personal Data (Administrator.Modify = True),**
  - **The Administrator is authenticated.**

FDP_ACF.1.3/Administration

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

FDP_ACF.1.4/Administration

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

FDP_UCT.1/SM Basic data exchange confidentiality

FDP_UCT.1.1/SM

The TSF shall enforce the **Administration SFP** to **transmit and receive** user data in a manner protected from unauthorized disclosure.

FDP_UIT.1/SM Data exchange integrity

FDP_UIT.1.1/SM

The TSF shall enforce the **Administration SFP** to **transmit and receive** user data in a manner protected from **modification, deletion, insertion and replay** errors.

FDP_UIT.1.2/SM

The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion or replay** has occurred.

FDP_ITC.1/Preparation Import of user data without security attributes

FDP_ITC.1.1/Preparation

The TSF shall enforce the **Preparation SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/Preparation

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

FDP_ITC.1.3/Preparation

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **imported user data are protected in integrity and confidentiality with SFRs FCS_COP.1/ENC and FCS_COP.1/MAC.**

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 security attributes: **integrityControlledData**.

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall: **increase counter of the Killcard file. If the maximum is reached the killcard is launched.**

Application Note: This feature is inherited from the platform.

7.1.5 Class FMT Management of TSF Data

FMT_MTD.1/Config_Counter Management of TSF Data

FMT_MTD.1.1/Config_Counter

The TSF shall restrict the ability to **configure** the **Key Usage Counter Limit and Retry Counter Limit** to **Personalization Agent.**

FMT_MTD.1/INI_ENA Management of TSF Data

FMT_MTD.1.1/INI_ENA

The TSF shall restrict the ability to **write** the **Initialization Data and Pre-personalization Data** to **the Pre-personalization Agent.**

Note: Please refer to F.ACW for details of the data written by the manufacturer.

FMT_MTD.1/KEY_WRITE Management of TSF Data

FMT_MTD.1.1/KEY_WRITE

The TSF shall restrict the ability to **write** the **Keys (all)** to **the Personalization Agent.**

FMT_MTD.1/KEY_READ Management of TSF Data

FMT_MTD.1.1/KEY_READ

The TSF shall restrict the ability to **read** the **secret keys (all)** to **none.**

FMT_MTD.1/LIFE-CYCLE Management of TSF Data

FMT_MTD.1.1/LIFE-CYCLE

The TSF shall restrict the ability to **switch** the **Life-Cycle** to **Pre-Personalization Agent (only from Pre-Perso to Perso) and Personalization Agent (only from Perso to Operational).**

FMT_MTD.1/SM_LVL Management of TSF data

FMT_MTD.1.1/SM_LVL The TSF shall restrict the ability to **set** the **allowed Secure Messaging level when performing Mutual Authenticate** to **the Personalization Agent**.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:

- **Initialization,**
- **Pre-personalization,**
- **Personalization,**
- **Administration.**

FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the roles

- **Manufacturer,**
- **Pre-Personalization Agent,**
- **Personalization Agent,**
- **Administrator**

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1

The TSF shall restrict the ability to **enable** the functions **seal creation function** to **Administrator**.

7.2 Security Assurance Requirements (SAR)

The assurance components for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented by taking the following component: ALC_DVS.2, AVA_VAN.5 and ALC_FLR.3.

Details on requested assurance family levels for TOE targeted product are given in §7.3.3.2.

Explanations on each one are given in [CC3] in dedicated chapter.

7.3 Security Requirements Rationale

7.3.1 Security Objectives for the TOE

OT.Card_Auth_Proof is implemented by:

- FCS_COP.1/Mutual-Auth defines the cryptographic functions for the Mutual Authentication and FCS_COP.1/Internal-Auth define the cryptographic functions to identify and authenticates the Vitale Card.
- FIA_UID.1, FIA_UAU.1, FIA_UAU.4 and FIA_UAU.5 define the requirements for the authentication and the operations that can be performed before the authentication of a user.

- FIA_AFL.1 defines the management of the authentication failure for Mutual Authentication and Internal Authentication (on-line and off-line).
- FIA_API.1 defines how the identity of the Vitale Card is proven by the TOE.

OT.Preparation is implemented by:

- FDP_ACC.1/Preparation and FDP_ACF.1/Preparation define the operations that the Pre-Personalization and the Personalization Agents are allowed to perform during Preparation Phase. Those are also enforced by FMT_MTD.1/KEY_WRITE for the writing of the keys, and FMT_MTD.1/LIFE-CYCLE for the switch of Life-Cycle.
- The Pre-Personalization Agent and Personalization Agent roles are maintained by FMT_SMF.1 and FMT_SMR.1.
- FIA_UID.1, FIA_UAU.1, FIA_UAU.4 and FIA_UAU.5 define the requirements for the authentication and the operations that can be performed before the authentication of a user.
- Authentication of the roles is defined with FCS_COP.1/GP_AUTH.
- Secure exchanges are defined by FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC and FDP_ITC.1/Preparation. Master keys are protected as defined by FCS_COP.1/GP_KEY_DEC and session keys are derived as defined by FCS_CKM.5/GP. Those session keys are then erased as defined FCS_CKM.6.

OT.ADMIN_Configuration is implemented by:

- FDP_ACC.1/Administration and FDP_ACF.1/Administration define the operations that the Administrator is allowed to perform.
- FMT_MOF.1 restricts the ability to generate Seals to Administrator role.
- FCS_COP.1/Seal is the SFR defining how to generate the Seals.
- FMT_MTD.1/KEY_READ Prohibits reading of secret keys by any role, directly upholding confidentiality and resistance to misuse.
- FMT_SMF.1 and FMT_SMR.1 support the Administrator role and functions related.

OT.Key_Usage_Counter is implemented by:

- FCS_CKM.3 Enforces per-key usage counters; keys become inaccessible at limit. This constrains key exposure and misuses.
- FMT_MTD.1/Config_Counter Restricts configuration of usage/retry limits to authorized role, ensuring governance over key usage required by OT.Key_Usage_Counter.

OT.AC_SM_Level is implemented by:

- FMT_MTD.1/SM_LVL permits to set the SM level required to access the sensitive data.

OT.Data_Int is implemented by:

- FDP_ACC.1/Administration and FDP_ACF.1/Administration Establish Administration SFP (Administrator, objects, operations) for controlled modifications/seal creation
- FDP_ACC.1/Preparation and FDP_ACF.1/Preparation Establish the Preparation SFP

scope (subjects/objects/operations), enabling precise enforcement needed.

- FMT_SMR.1 lists the roles (including Personalization Agent)
- FMT_SMF.1 lists the TSF management functions (including Personalization).
- FMT_MTD.1/KEY_WRITE limits the ability to write the keys to the Personalization Agent.
- FIA_UAU.4.1 and FIA_UAU.5.1 for authentication of the Terminal as Personalization Agent.
- FIA_UAU.5, FDP_UCT.1/SM and FDP_UIT.1/SM requires the protection of the transmitted data by means of secure messaging implemented by the cryptographic functions according to FCS_COP.1/SM, FCS_RNG.1, and FCS_COP.1/GP_ENC and FCS_COP.1/GP_MAC for the ENC and MAC
- FDP_SDI.2 ensures detection of integrity errors
- FPT_PHP.3 ensures physical resistance against tampering and probing, protecting TOE and its data.
- FPT_TST.1 conducts integrity tests to detect any unauthorized tampering.
- FPT_FLS.1 On failures (tearing, power/clock/temp, integrity), preserves secure state, limiting security impact.

OT.Data_Conf is implemented by:

- FCS_CKM.5/GP Derives GP session keys, enabling confidentiality/integrity of GP exchanges during preparation.
- FCS_CKM.5/SM Derives SM session keys, required Secure Messaging level, thereby enforcing OT.Data_Conf for operational communications.
- FCS_COP.1/GP_ENC Provides AES-CBC encryption for GP SM such that imported and or personalization data remain confidential.
- FCS_COP.1/GP_MAC Provides AES CMAC for GP messaging integrity/authenticity to prevent unauthorized modification during preparation.
- FCS_COP.1/SM Enforces AES-CMAC protected APDUs under SM; required SM level gating read access.
- FDP_ITC.1/Preparation Ensures imported user data are protected in integrity/confidentiality and external attributes are ignored.
- FDP_UCT.1/SM Confidentiality of user data in transit under Administration SFP, meeting the confidentiality aspects of OT.Data_Conf.
- FDP_UIT.1/SM Integrity and anti-replay for user data in transit under Administration SFP.
- FPT_EMS.1 Prevents leakage of information

OT.Identification is implemented by:

- FIA_UAU.1 Defines authentication preconditions; only authenticated entities may perform TSF-mediated actions.
- FIA_UID.1 Defines identification preconditions; restricts actions prior to identification to a safe subset.
- FMT_MTD.1/INI_ENA Restricts writing of Initialization/Pre-personalization data to Manufacturer.

- FMT_SMF.1 Defines the authoritative set of management functions, bounding administrative surface to what OT.Identification permits.
- FMT_SMR.1 Defines roles (Manufacturer, Pre-/Personalization Agents, Administrator) on which SFP decisions rely.

OT.Prot_Abuse-Func is implemented by:

- FDP_ACC.1/Administration Establishes Administration SFP (Administrator, objects, operations) for controlled modifications/seal creation.
- FDP_ACF.1/Administration Enforces rules for read/modify/seal in Operational state with required attributes, preventing misuse.
- FMT_MTD.1/KEY_READ Prohibits reading of secret keys by any role, directly upholding confidentiality and resistance to misuse.
- FMT_SMF.1 Defines the authoritative set of management functions.
- FMT_SMR.1 Defines roles (Manufacturer, Pre-/Personalization Agents, Administrator) on which SFP decisions rely .
- FPT_FLS.1 On failures (tearing, power/clock/temp, integrity), preserves secure state
- FPT_PHP.3 Physical probing/manipulation elicits automatic responses that keep SFRs enforced
- FPT_TST.1 Self-tests at reset and authorized integrity checks detect corruption

OT.Prot_Inf_Leak is implemented by:

- FPT_EMS.1 Constrains emanations across attack surfaces (e.g., power variation at contact interface) so they do not disclose TSF/user data.
- FPT_FLS.1 On failures (tearing, power/clock/temp, integrity), preserves secure state, limiting security impact.
- FPT_PHP.3 Physical probing/manipulation elicits automatic responses that keep SFRs enforced; protects keys confidentiality.
- FPT_TST.1 Self-tests at reset and authorized integrity checks detect corruption, helping maintain trustworthy operation consistent

OT.Tamper_Resistance is implemented by:

- FPT_PHP.3 Physical probing/manipulation elicits automatic responses that keep SFRs enforced; protects keys.

OT.Prot_Malfunction is implemented by:

- FPT_FLS.1 On failures (tearing, power/clock/temp, integrity), preserves secure state, limiting security impact.
- FPT_TST.1 Self-tests at reset and authorized integrity checks detect corruption, helping maintain trustworthy operation consistent.

OT.Crypto is implemented by:

- FCS_RNG.1 ensures that the Random Numbers are generated with a sufficient security level.
- FCS_CKM.5/GP and FCS_CKM.5/SM ensure that session keys are generated with sufficient security level.
- FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_KEY_DEC, FCS_COP.1/Seal, FCS_COP.1/Mutual-Auth, FCS_COP.1/SM, FCS-COP.1/Internal-Auth implement standardized algorithms following [PG-083] recommendations.

7.3.2 SFRs and Security Objectives OT – Coverage

SFR	OT
FCS_RNG.1	OT.Crypto
FCS_CKM.5/GP	OT.Preparation ; OT.Data_Conf ; OT.Crypto; OT.Data_In
FCS_COP.1/GP_ENC	OT.Preparation ; OT.Data_Conf ; OT.Crypto; OT.Data_In
FCS_COP.1/GP_MAC	OT.Preparation ; OT.Data_Conf ; OT.Crypto; OT.Data_In
FCS_COP.1/GP_AUTH	OT.Preparation ; OT.Crypto
FCS_COP.1/GP_KEY_DEC	OT.Preparation ; OT.Crypto
FCS_COP.1/Seal	OT.ADMIN_Configuration ; OT.Crypto
FCS_COP.1/Mutual-Auth	OT.Card_Auth_Proof ; OT.Crypto
FCS_COP.1/SM	OT.Data_Conf ; OT.Crypto
FCS_COP.1/Internal-Auth	OT.Card_Auth_Proof ; OT.Crypto
FCS_CKM.5/SM	OT.Data_Conf ; OT.Crypto
FCS_CKM.3	OT.Key_Usage_Counter ;
FCS_CKM.6	OT.Preparation ;
FIA_UID.1	OT.Preparation ; OT.Identification ; OT.Card_Auth_Proof
FIA_UAU.1	OT.Preparation ; OT.Identification ; OT.Card_Auth_Proof
FIA_UAU.4	OT.Preparation ; OT.Card_Auth_Proof ; OT.Data_Int
FIA_UAU.5	OT.Preparation ; OT.Card_Auth_Proof ; OT.Data_Int
FIA_AFL.1	OT.Card_Auth_Proof
FIA_API.1	OT.Card_Auth_Proof
FPT_EMS.1	OT.Prot_Inf_Leak ; OT.Data_Conf
FPT_TST.1	OT.Prot_Inf_Leak ; OT.Prot_Malfunction ; OT.Data_Int ; OT.Prot_Abuse-Func ;
FPT_FLS.1	OT.Prot_Inf_Leak ; OT.Prot_Malfunction ; OT.Prot_Abuse-Func ; OT.Data_Int;
FPT_PHP.3	OT.Prot_Inf_Leak ; OT.Tamper_Resistance ; OT.Data_Int ; OT.Prot_Abuse-Func
FDP_ACC.1/Preparation	OT.Preparation ; OT.Data_Int
FDP_ACF.1/Preparation	OT.Preparation ; OT.Data_Int

FDP_ACC.1/Administration	OT.ADMIN_Configuration ; OT.Prot_Abuse-Func ; OT.Data_Int
FDP_ACF.1/Administration	OT.ADMIN_Configuration ; OT.Data_Int ; OT.Prot_Abuse-Func
FDP_UCT.1/SM	OT.Data_Conf ; OT.Data_Int
FDP_UIT.1/SM	OT.Data_Conf ; OT.Data_Int
FDP_ITC.1/Preparation	OT.Preparation ; OT.Data_Conf
FDP_SDI.2	OT.Data_Int
FMT_MTD.1/Config_Counter	OT.Key_Usage_Counter
FMT_MTD.1/INI_ENA	OT.Identification
FMT_MTD.1/KEY_WRITE	OT.Preparation ; OT.Data_Int
FMT_MTD.1/KEY_READ	OT.Prot_Abuse-Func; OT.ADMIN_Configuration
FMT_MTD.1/LIFE-CYCLE	OT.Preparation ;
FMT_MTD.1/SM_LVL	OT.AC_SM_Level;
FMT_SMF.1	OT.ADMIN_Configuration ; OT.Preparation ; OT.Identification ; OT.Prot_Abuse-Func ; OT.Data_Int
FMT_SMR.1	OT.ADMIN_Configuration ; OT.Preparation ; OT.Identification ; OT.Prot_Abuse-Func ; OT.Data_Int
FMT_MOF.1	OT.ADMIN_Configuration

Table 6 SFRs and Security Objectives OT – Coverage

OT	SFR
OT.AC_SM_Level	FMT_MTD.1/SM_LVL ;
OT.ADMIN_Configuration	FDP_ACC.1/Administration; FDP_ACF.1/Administration; FMT_MOF.1; FCS_COP.1/Seal; FMT_MTD.1/KEY-READ; FMT_SMF.1; FMT_SMR.1
OT.Card_Auth_Proof	FCS_COP.1/Internal-Auth; FCS_COP.1/Mutual-Auth; FIA_AFL.1; FIA_API.1; FIA_UAU.1; FIA_UAU.4; FIA_UAU.5; FIA_UID.1
OT.Data_Conf	FCS_CKM.5/GP; FCS_CKM.5/SM; FCS_COP.1/GP_ENC; FCS_COP.1/GP_MAC; FCS_COP.1/SM; FDP_ITC.1/Preparation; FDP_UCT.1/SM; FDP_UIT.1/SM; FPT_EMS.1
OT.Data_Int	FDP_ACC.1/Administration; FDP_ACF.1/Administration; FDP_ACC.1/Preparation; FDP_ACF.1/Preparation; FMT_SMR.1; FMT_SMF.1; FMT_MTD.1/KEY_WRITE; FIA_UAU.4; FIA_UAU.5, FDP_UCT.1/SM; FDP_UIT.1/SM; FCS_COP.1/SM, FCS_RNG.1; FCS_COP.1/GP_ENC; FCS_COP.1/GP_MAC; FDP_SDI.2; FPT_PHP.3; FPT_TST.1; FPT_FLS.1;

OT	SFR
OT.Identification	FIA_UAU.1;FIA_UID.1;FMT_MTD.1/INI_ENA;FMT_SMF.1;FMT_SMR.1;
OT.Key_Usage_Counter	FCS_CKM.3; FMT_MTD.1/Config_Counter;
OT.Preparation	FCS_CKM.5/GP; FCS_CKM.6; FCS_COP.1/GP_AUTH; FCS_COP.1/GP_ENC; FCS_COP.1/GP_KEY_DEC; FCS_COP.1/GP_MAC; FDP_ACC.1/Preparation; FDP_ACF.1/Preparation; FDP_ITC.1/Preparation; FIA_UAU.1; FIA_UAU.4; FIA_UAU.5; FIA_UID.1; FMT_MTD.1/LIFE-CYCLE; FMT_MTD.1/KEY_WRITE; FMT_SMF.1; FMT_SMR.1
OT.Prot_Abuse-Func	FDP_ACC.1/Administration; FDP_ACF.1/Administration; FMT_MTD.1/KEY_READ; FMT_SMF.1; FMT_SMR.1; FPT_FLS.1; FPT_PHP.3; FPT_TST.1;
OT.Prot_Inf_Leak	FPT_EMS.1; FPT_FLS.1; FPT_PHP.3; FPT_TST.1
OT.Prot_Malfunction	FPT_FLS.1; FPT_TST.1;
OT.Tamper_Resistance	FPT_PHP.3
OT.Crypto	FCS_RNG.1; FCS_CKM.5/GP; FCS_CKM.5/SM; FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC, FCS_COP.1/GP_AUTH, FCS_COP.1/GP_KEY_DEC, FCS_COP.1/Seal, FCS_COP.1/Mutual-Auth, FCS_COP.1/SM, FCS-COP.1/Internal-Auth

Table 7 Security Objectives OT and SFRs – Coverage

7.3.3 Dependencies

7.3.3.1 SFRs dependencies

Requirements	CC dependencies	Satisfied dependencies
FCS_RNG.1	No dependencies	
FCS_CKM.5/GP	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.6	FCS_COP.1/GP_ENC, FCS_COP.1/GP_MAC Dependency to FCS_CKM.6 is not satisfied because these keys are automatically erased when the card resets.
FCS_COP.1/GP_ENC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] and FCS_CKM.6	FCS_CKM.5/GP Dependency to FCS_CKM.6 is not satisfied because these keys are automatically erased when the card resets.
FCS_COP.1/GP_MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] and FCS_CKM.6	FCS_CKM.5/GP Dependency to FCS_CKM.6 is not satisfied because these keys are

Requirements	CC dependencies	Satisfied dependencies
		automatically erased when the card resets.
FCS_COP.1/GP_AUTH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] and FCS_CKM.6	FDP_ITC.1/Preparation Dependency to FCS_CKM.6 is not satisfied because the keys are never removed.
FCS_COP.1/GP_KEY_DEC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] and FCS_CKM.6	FDP_ITC.1/Preparation Dependency to Import of the keys protection FCS_CKM.6 is not satisfied because the keys are never removed.
FCS_COP.1/Seal	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] and FCS_CKM.6	FDP_ITC.1/Preparation Dependency to FCS_CKM.6 is not satisfied because the keys are never removed.
FCS_COP.1/Mutual-Auth	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] and FCS_CKM.6	FDP_ITC.1/Preparation Dependency to FCS_CKM.6 is not satisfied because the keys are never removed.
FCS_COP.1/SM	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] and FCS_CKM.6	FCS_CKM.5/SM FCS_CKM.6
FCS_COP.1/Internal-Auth	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] and FCS_CKM.6	FDP_ITC.1/Preparation Dependency to FCS_CKM.6 is not satisfied because the keys are never removed.
FCS_CKM.5/SM	[FCS_CKM.2 or FCS_COP.1] and FCS_CKM.6	FCS_COP.1/SM FCS_CKM.6
FCS_CKM.3	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	FDP_ITC.1/Preparation FCS_CKM.5/GP FCS_CKM.5/SM
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	FCS_CKM.5/SM
FIA_UID.1	No dependencies	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.4	No dependencies	
FIA_UAU.5	No dependencies	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_API.1	No dependencies	

Requirements	CC dependencies	Satisfied dependencies
FPT_EMS.1	No dependencies	
FPT_TST.1	No dependencies	
FPT_FLS.1	No dependencies	
FPT_PHP.3	No dependencies	
FDP_ACC.1/Preparation	FDP_ACF.1	FDP_ACF.1/Preparation
FDP_ACF.1/ Preparation	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1/Preparation The security attributes used in FDP_ACF.1/Preparation are related to the authentication of the role. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.
FDP_ACC.1/Administration	FDP_ACF.1	FDP_ACF.1/Administration
FDP_ACF.1/ Administration	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.1/Administration The security attributes used in FDP_ACF.1/Administration are defined during the personalization and cannot be modified or depends on authentication of a user. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary here.
FDP_UCT.1/SM	[FTP_ITC.1 or FTP_TRP.1] and [FDP_ACC.1 or FDP_IFC.1]	Dependency to FTP_ITC.1 or FTP_TRP.1 are not satisfied. There is only one communication channel (so no need of FTP_ITC.1) and since the TOE does not provide a direct human interface a trusted path as required in FTP_TRP.1 is not applicable here. FDP_ACC.1/Administration
FDP_UIT.1/SM	[FDP_ACC.1 or FDP_IFC.1] and [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1/Administration Dependency to FTP_ITC.1 or FTP_TRP.1 are not satisfied. There is only one communication channel (so no need of FTP_ITC.1) and since the TOE does not provide a direct human interface a trusted

Requirements	CC dependencies	Satisfied dependencies
		path as required in FTP_TRP.1 is not applicable here.
FDP_ITC.1/Preparation	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/Preparation The security attributes used in SFP Preparation are related to the authentication of the role. No management of these security attributes (i.e. SFR FMT_MSA.3) is necessary here.
FDP_SDI.2	No dependencies	
FMT_MTD.1/Config_Counter	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1/KEY_WRITE	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1/KEY_READ	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1/LIFE-CYCLE	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1/SM_LVL	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1

7.3.3.2 SARs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.3, ALC_TAT.1
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	

ALC_FLR.3	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

7.3.4 Rationale for the Security Assurance Requirements

The assurance level for this Security Target is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. Augmentation results from the selection of following SAR.

7.3.4.1 AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to function with a variety of seal creation systems Due to the nature of its intended applications, i.e. the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. Insecure states shall be easy to detect and the TOE shall be shown to be highly resistant to penetration attacks to protect the integrity of sensitive information stored in the TOE, the confidentiality if the keys used by the TOE and ensure a sufficient level of security for authentication and data sealing mechanisms.

7.3.4.2 ALC_DVS.2 Sufficiency of security measures

In order to protect the TOE on development Phase, the component ALC_DVS.2 was added. This latter requires security documentation justifying that the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.

7.3.4.3 ALC_FLR.3 Systematic flaw remediation

The flaw remediation assurance improves a rigorous management for updating the TOE in the context of sensible market.

8 Composition with Platform Security Target

The underlying JavaCard open platform is certified at level EAL 6 augmented with ALC_FLR.3. As such it complies with the evaluation level assurance of the composite TOE.

8.1 Compatibility between TOE and Platform Threats

8.1.1 Confidentiality

T.CONFID-APPLI-DATA

The attacker executes an application to disclose data belonging to another application.

➔ All Threats

T.CONFID-JCS-CODE

The attacker executes an application to disclose the Java Card System code.

➔ No contradiction

T.CONFID-JCS-DATA

The attacker executes an application to disclose data belonging to the Java Card System.

➔ No contradiction

8.1.2 Integrity

T.INTEG-APPLI-CODE

The attacker executes an application to alter (part of) its own code or another application's code.

➔ All threats

T.INTEG-APPLI-CODE.LOAD

The attacker modifies (part of) its own or another application code when an application package is transmitted to the card for installation.

➔ No contradiction and concerns also all threats

T.INTEG-APPLI-DATA

The attacker executes an application to alter (part of) another application's data.

➔ All threats

T.INTEG-APPLI-DATA.LOAD

The attacker modifies (part of) the initialization data contained in an application package when the package is transmitted to the card for installation.

➔ All threats

T.INTEG-JCS-CODE

The attacker executes an application to alter (part of) the Java Card System code.

➔ No contradiction

T.INTEG-JCS-DATA

The attacker executes an application to alter (part of) Java Card System or API data.

➔ No contradiction

8.1.3 Identity usurpation

T.SID.1

An applet impersonates another application, or even the Java Card RE, in order to gain illegal access to some resources of the card or with respect to the end user or the terminal.

➔ No contradiction

T.SID.2

The attacker modifies the TOE's attribution of a privileged role (e.g. default applet and currently selected applet), which allows illegal impersonation of this role.

➔ No contradiction

8.1.4 Unauthorized execution

T.EXE-CODE.1

An applet performs an unauthorized execution of a method.

➔ No contradiction, this threat concerns also all application Threats

T.EXE-CODE.2

An applet performs an execution of a method fragment or arbitrary data.

➔ No contradiction, this threat concerns also all application Threats

T.NATIVE

An applet executes a native method to bypass a TOE Security Function such as the firewall. See #.NATIVE for details.

➔ No contradiction

8.1.5 Denial of service

T.RESOURCES

An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM.

➔ No contradiction

8.1.6 Card management

T.DELETION

The attacker deletes an applet or a package already in use on the card, or uses the deletion functions to pave the way for further attacks (putting the TOE in an insecure state).

➔ No contradiction

T.INSTALL

The attacker fraudulently installs post-issuance of an applet on the card. This concerns either the installation of an unverified applet or an attempt to induce a malfunction in the TOE through the installation process. .

➔ No contradiction

8.1.7 Services

T.OBJ-DELETION

The attacker keeps a reference to a garbage collected object in order to force the TOE to execute an unavailable method, to make it to crash, or to gain access to a memory containing data that is now being used by another application.

➔ All threats

8.1.8 Miscellaneous

T.PHYSICAL

The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (opposed to logical) tampering means. This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA. That also includes the modification of the runtime execution of Java Card System or SCP software through alteration of the intended execution order of (set of) instructions through physical tampering techniques.

➔ T.Phys-Tamper

8.1.9 Additional threats

T.CONFIGURATION

The attacker tries to observe or modify configuration information exchanged between the TOE and its environment. The TOE in this phase must protect itself from modification or theft. Even the field is protected by assurance measures, each operations realised in this phase has to be protected.

➔ All threats

T.CONF_DATA_APPLET

The attacker tries to observe the operation of comparison between two byte arrays in order to catch confidential information manipulated.

➔ All threats

T.PATCH_LOADING

The attacker tries to avoid the loading of a genuine patch, alter a patch (during loading or once loaded), or to exploit the patch loading mechanism to load unauthenticated code on the TOE, in order to get access to the assets, the TSF data or the TOE user data, or to modify the TF.

➔ No contradiction

8.2 Coverage of the Assumptions of the Javacard Open Platform (A.PLT vs TOE)

Assumption of platform	Rationale
A.CAP_FILE	CAP Files loaded post-issuance do not contain native methods. The Java Card specification explicitly "does not include support for native methods" ([JC]) outside the API.
A.VERIFICATION	This assumption is upheld by OE.VERIFICATION and OE.CODE_EVIDENCE. These objectives are fulfilled by the applet included in the TOE (see §8.4). For the other applet that may be loaded on the TOE, it is covered by recommendations in [PTF_AGD_OPE] whose fulfilment shall be verified by the risk manager.

8.3 Coverage of the OSP of the Javacard Open Platform (OSP.PLT vs TOE)

OSP of platform	Rationale
OSP.VERIFICATION	This OSP is upheld by OE.VERIFICATION and OE.CODE_EVIDENCE. These objectives are fulfilled by the applet included in the TOE (see §8.4). For the other applet that may be loaded on the TOE, it is covered by recommendations in IC whose fulfilment shall be verified by the risk manager.

8.4 Coverage of the security objective of the Javacard Open Platform Environment (OE.PLT vs TOE)

Security objective of platform environment	Rationale
OE.CAP_FILE	No Native API can be nested within Applet loaded in post issuance as the platform only allows the loading of javacard bytecode (only at pre-issuance).

OE.VERIFICATION	This objective is fulfilled by loaded applets in the TOE.
OE.CODE-EVIDENCE	This objective is fulfilled by the applet included in the TOE. The applet is verified then included in the generated platform in IN Smart Identity facilities. For the other applet that may be loaded on the TOE, it is covered by recommendations in [PTF_AGD_OPE] whose fulfilment shall be verified by the risk manager

9 TOE Summary Specification

9.1 TOE Summary Specification

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions.

The security functionalities concerning the IC and the JC Platform are described in [ST-IC], [ST-PL] and are not redefined in this security target, although they must be considered for the TOE.

9.1.1 IC security functions

The full list of the IC Platform security functionalities can be checked in the IC Platform Security Target [ST-IC].

9.1.2 Platform security functions

The full list of the JC Platform security functionalities can be checked in the JC Platform Security Target [ST-PL].

9.1.3 Vitale security functions

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions.

F.AUTH - Authentication

Only authenticated CAC can get access to the TOE (user data stored and updates on the Vitale card). The Vitale card offers several authentication mechanisms to authenticate different actors:

- Reader terminals or on healthcare professional workstations using (**Symmetric Internal Authentication)**
- Same as above but the Authentication is done by an offline terminal using asymmetric keys (**Asymmetric Internal Authentication**)
- Card Administration Channel (CAC): **Mutual Authentication** is necessary for the Administrator to access the Vitale card
- Pre-Personalization and Personalization Agents are authenticated using **GP authentication**.

Authentication is necessary for all users:

- Pre-Personalization Agent
- Personalization Agent
- Administrator

F.SM - Secure Messaging

This security functionality ensures the confidentiality, authenticity and integrity of the communication between the TOE and the interface device. In the operational phase, after a successful Mutual Authentication Procedure, a secure channel is established. This security functionality also provides a Secure Messaging (SCP03) for the transmission of user data in Pre-personalization and Personalization phases. The protocols can be configured to protect the exchanges integrity and/or confidentiality. If an error occurs in the secure messaging layer or if the session is closed, the session keys are destroyed. Also, the use of challenges enforces a protection against replay.

A Secure Messaging level is associated to sensitive data, allowing different access control depending on this level. Only the Personalization Agent can modify this Secure Message level.

F.ACW - Access Control in Writing

This security function controls access to write functions (in NVM) and enforces the security policy for data writing and updating. Prior to any data update, it authenticates the actor (F.AUTH), opens a Secure Messaging (F.SM) and checks the access conditions are fulfilled as well as the life cycle state.

At preparation stage:

- Pre-Personalization Agent can write Pre-personalization data and Perso Agent Keys.
- Personalization Agent can write all the objects (EFs, DO/SDOs). This role is in charge of writing SM Keys, Seal/Signature Keys, Authenticity of the Vitale card data, Personal Data of the End user, and Seal Creation security attributes (FDP_ACC.1 and FDP_ACF.1)

At operational stage:

- It is not possible to create any files (system or data files).
- Administrator with correct access rights (security attribute “modify” = True) can update the End user information (Personal data).

F.ACR - Access Control in Reading

This security function controls access to read functions and enforces the security policy for data retrieval. Prior to any data retrieval, it authenticates the actor (F.AUTH) trying to access the objects (EFs, DO/SDOs), opens a Secure Messaging (F.SM) and checks the access conditions are fulfilled as well as the life cycle state.

It ensures that at any time, keys are never readable.
In the Operational Use phase:

- The terminal can read Personal Data.

In the Production and preparation stage:

- The Manufacturer can read the Initialization Data in *Stage 2* “Production” (see §2.2).
- The Personalization Agent can read Personal data after he is authenticated by the TOE.

It ensures as well that no other part of the memory can be accessed at any time.

F.PHY - Physical Protection

This security function protects the TOE against physical attacks, so that the integrity and confidentiality of the TOE is ensured, including keys, user data, configuration data and TOE life cycle. It performs self-testing, detects physical tampering, responds automatically, and also controls the emanations sent out by the TOE.

This security function also limits any physical emanations from the TOE so as to prevent any information leakage via these emanations that might reveal or provide access to sensitive data.

F.PREP - Pre-personalization

This security functionality is performed only after the authentication of the Pre-Personalization Agent with a Mutual Authenticate mechanism (F.AUTH) and the opening of a Secure Channel according to [GPC_SPE_014] (F.SM).

This security function allows to:

- Initialization of the TOE,
- Load Personalization Agent keys in encrypted form,
- Store the Pre-Personalization data in audit records.
- Configuration of counters values (key usage and retry counter)
- Set TOE life cycle to Personalization phase.

F.PERSO – Personalization

This security functionality is performed only after the authentication of the Personalization Agent with a Mutual Authenticate mechanism (F.AUTH) and the opening of a Secure Channel (F.SM).

This security function allows to:

- Write SM Keys, Seal/Signature Keys, Authenticity of the Vitale card data, Personal Data of the End user, and Seal Creation security attributes,
- Set TOE life cycle to Operational Use phase.

F.SS - Safe State Management

This security functionality ensures that the TOE gets back to a secure state when:

- a tearing occurs (during a copy of data in NVM),
- an error due to self-test as defined in FPT_TST.1,
- any physical tampering is detected.

This security function ensures that if such a case occurs, the TOE either is switched in the state "kill card" or becomes mute, only audit traceability is possible.

F.ADMIN - Administration

This security functionality is performed only after the authentication of the Admin Agent with a Mutual Authenticate mechanism (F.AUTH) and the opening of a Secure Channel (F.SM).

Depending on the Admin access rights:

- If the Admin has the security attribute “Modify”, he is allowed to modify Personal Data.

- If the Admin has the security attribute “Seal Creation”, he can send DTBS and request Seal creation. DTBS is protected in integrity by the TOE during the process.

F.CRYPTO - Cryptographic Support

This security function provides the following cryptographic features:

- Session Key generation for AES with key sizes 128 and 256 bits.
- Secure messaging (encryption and decryption) using:
  - AES in CBC mode (key sizes 128 and 256 bits)
- Secure messaging (message authentication code) using:
  - AES CMAC with key sizes 128 and 256 bits
- Symmetric Authentication - encryption and decryption using:
  - AES CMAC with key sizes 128 and 256 bits as defined in [NIST_800_38B].
- Key decryption using:
  - AES in CBC mode with key sizes 128 and 256 bits as defined in [FIPS_197]

F.RATIF – Retry Counter

A counter is associated with an SDO which is used to count the number of successive unsuccessful authentication attempts. The counter is initialized when the authentication is successful. If the counter reaches its maximum value, then the related secret is blocked and cannot be used anymore.

F.RATIF_K_Usage – Key Usage Counter

A usage counter is associated with an SDO which is used to count the number of times the SDO has been used. An SDO with an initial usage counter of N can be used N successful times. Once the value 0 is reached, the object is blocked.

F.APP_INTEGRITY

This security functionality monitors the integrity of sensitive data (Retry counters, Key Usage counters, private and secret keys, access conditions of created objects, etc.). The integrity of persistently stored data such as symmetric and asymmetric keys is monitored using the JC Platform features (see [ST-PL]). In case of integrity error this TSF will:

- Prohibit the use of the altered data, and
- Inform the Admin about integrity error.

9.2 SFR and TSS - Rationale

TSS	SFRs	Rationale
F.AUTH – Authentication	FCS_COP.1/GP_AUTH FCS_COP.1/Mutual-Auth FCS_COP.1/Internal-Auth FIA_UAU.1 FIA_UAU.4 FIA_UAU.5 FIA_AFL.1	GP authentication is managed through FCS_COP.1/GP_AUTH. FIA_UAU.4 and FIA_UAU.5 enforce authentication limits, while FIA_AFL.1 handles authentication failures. FCS_COP.1/Mutual-Auth provide an authentication mechanism to ensure

TSS	SFRs	Rationale
	FIA_UID.1 FIA_API.1	authenticity of the actors involved in the authentication process (Administrator and Vitale card). FIA_API.1 requires that the Vitale card is able to authenticate itself. FCS_COP.1/Internal-Auth is the cryptographic mechanism allowing the Vitale card to authenticate itself either with symmetric crypto (online) or asymmetric crypto (offline). FIA_UID.1 and FIA_UAU.1 define the operations authorized before the identification/authentication of the users and requires all users to be authenticated before performing any other actions.
F.SM – Secure Messaging	FCS_CKM.5/GP FCS_COP.1/GP_ENC FCS_COP.1/GP_MAC FCS_COP.1/SM FCS_CKM.5/SM FCS_CKM.6 FDP_UCT.1/SM FDP_UIT.1/ SM FCS_COP.1/GP_ENC FCS_COP.1/GP_MAC FDP_ITC.1/Preparation FMT_MTD.1/SM_LVL	FCS_CKM.5/GP derives GP Session Keys used for the GP Secure Messaging. FCS_COP.1/GP_ENC and FCS_COP.1/GP_MAC define how the GP Secure Messaging protects the exchanges in integrity and confidentiality. FCS_COP.1/SM ensures secure communication between TOE and the interface device through secure messaging using Session SM keys. FCS_CKM.5/SM derives Session SM keys, ensuring secure key exchange for communications. FCS_CKM.6 is used to erase Secure Messaging keys. FDP_UIT.1/SM and FDP_UCT.1 define the confidentiality and integrity properties of the Secure Messaging. FDP_ITC.1/Preparation enforces the rules to protect the import of user data during Preparation phase. Secure Messaging is associated to a level which defines access control on sensitive data, as defined in FMT_MTD.1/SM_LVL.
F.ACW – Access Control in Writing	FDP_ACC.1/Preparation FDP_ACF.1/Preparation FDP_ACC.1/Administration FDP_ACF.1/Administration FMT_MTD.1/Config_Counter FMT_MTD.1/KEY_WRITE FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/Preparation and FDP_ACF.1/Preparation define the rules for writing Pre-Personalization and Personalization data in Preparation stage. FMT_MTD.1/KEY_WRITE limits the ability to write the keys to the Personalization Agent. FDP_ACC.1/Preparation and FDP_ACF.1/Preparation define the rules for

TSS	SFRs	Rationale
		modifying Personal Data in Operational phase. FMT_MTD.1/Config_Counter limits the ability to configure the counters limits to Personalization Agent. FDP_ACC.1/Administration and FDP_ACF.1/Administration ensure that only authorized users can modify security-sensitive data objects, implementing proper access control in writing. FMT_SMR.1 and FMT_SMF.1 define the roles and management functions controlling write access to critical data in the NVM.
F.ACR – Access Control in Reading	FMT_MTD.1/KEY_READ FDP_ACC.1/Preparation FDP_ACF.1/Preparation FDP_ACC.1/Administration FDP_ACF.1/Administration FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/Preparation and FDP_ACF.1/Preparation define the rules for reading Personal Data during the Preparation phases. FMT_MTD.1/KEY_READ ensures that nobody can read sensitive keys. FDP_ACC.1/Administration and FDP_ACF.1/Administration ensure that only the authorized and authenticated users can read Personal Data. FMT_SMR.1 and FMT_SMF.1 define the roles and management functions controlling write access to critical data in the NVM.
F.PHY – Physical Protection	FPT_PHP.3 FPT_EMS.1 FPT_FLS.1 FPT_TST.1	FPT_PHP.3 ensures physical resistance against tampering and probing, protecting TOE and its data. FPT_EMS.1 mitigates physical emanations that could lead to information leakage. FPT_FLS.1 ensures a secure state if any physical tampering or error is detected, while FPT_TST.1 conducts integrity tests to detect any unauthorized tampering.
F.PREP – Pre-personalization	FDP_ACC.1/Preparation FDP_ACF.1/Preparation FMT_SMR.1 FMT_SMF.1 FDP_ITC.1/Preparation FMT_MTD.1/LIFE-CYCLE FMT_MTD.1/INI_ENA	FDP_ACC.1/Preparation and FDP_ACF.1/Preparation define the rules for writing and reading Pre-Personalization data. FMT_SMR.1 and FMT_SMF.1 define the roles and management functions regarding Pre-Personalization stage. FDP_ITC.1/Preparation enforces the rules to protect the import of user data during Pre-Personalization. FMT_MTD.1/LIFE-CYCLE defines that only the Pre-personalization Agent can switch the Life-cycle state from Pre-Perso to Perso.

TSS	SFRs	Rationale
		FMT_MTD.1/INI_ENA defines that only Pre-Personalizer can write Initialization Data and Pre-personalization Data
F.PERSO – Personalization	FDP_ACC.1/Preparation FDP_ACF.1/Preparation FMT_SMR.1 FMT_SMF.1 FMT_MTD.1/Config_Counter FMT_MTD.1/KEY_WRITE FDP_ITC.1/Preparation FMT_MTD.1/LIFE-CYCLE FMT_MTD.1/SM_LVL	FDP_ACC.1/Preparation and FDP_ACF.1/Preparation define the rules for writing and reading Personalization data. FMT_SMR.1 and FMT_SMF.1 define the roles and management functions regarding Personalization stage. FMT_MTD.1/Config_Counter limits the configuration of the counters' limits and FMT_MTD.1/KEY_WRITE limits the writing of the keys to Personalization Agent. FDP_ITC.1/Preparation enforces the rules to protect the import of user data during Personalization. FMT_MTD.1/LIFE-CYCLE defines that only the Personalization Agent can switch the Life-cycle state from Perso to Operational. Only the Personalization Agent can modify the SM Level of a sensitive data, as defined in FMT_MTD.1/SM_LVL
F.SS – Safe State Management	FPT_FLS.1 FPT_TST.1 FPT_PHP.3	FPT_FLS.1 ensures the TOE returns to a secure state in case of an error. FPT_TST.1 verifies the integrity of the system at reset, while FPT_PHP.3 prevents unauthorized access or modifications, ensuring that the system remains secure even during malfunctions or tampering.
F.ADMIN – Administration	FDP_ACC.1/Administration FDP_ACF.1/Administration FCS_COP.1/Seal FMT_SMF.1 FMT_SMR.1 FMT_MOF.1	FDP_ACC.1/Administration and FDP_ACF.1/Administration defines the conditions for an Administrator to generate a Seal, modify Personal Data or read Personal data. FMT_SMR.1 and FMT_SMF.1 define the roles and management functions regarding Operational stage. FMT_MOF.1 restricts the ability to generate Seals to Administrator role. FCS_COP.1/Seal is the SFR defining how to generate the Seals.
F.CRYPTO – Cryptographic Support	FCS_RNG.1 FCS_CKM.5/GP FCS_COP.1/GP_ENC FCS_COP.1/GP_MAC FCS_COP.1/GP_AUTH	FCS_RNG.1 defines the random number generation requirements. All the Vitale Keys loaded in Perso are sent ciphered and can be deciphered with FCS_COP.1/GP_KEY_DEC.

TSS	SFRs	Rationale
	FCS_COP.1/GP_KEY_DEC FCS_COP.1/Seal FCS_COP.1/SM FCS_COP.1/Mutual-Auth FCS_CKM.5/SM FCS_COP.1/Internal-Auth FCS_CKM.3 FCS_CKM.6	Regarding GP authentication and Secure Messaging, FCS_COP.1/GP_AUTH is in charge of the authentication of the Pre-Perso or Perso Agent, FCS_CKM.5/GP is in charge of generating the GP Session Keys, FCS_COP.1/GP_ENC is in charge of protecting the exchanges in confidentiality and FCS_COP.1/GP_MAC in integrity. FCS_COP.1/Seal is in charge of generating a Seal on Administrator request. FCS_COP.1/Mutual-Auth allows to mutually authenticate the Vitale Card and the Administrator. Once this step is validated, FCS_CKM.5/SM generates SM Session keys to protect the next exchanges in confidentiality and integrity thanks to FCS_COP.1/SM. FCS_COP.1/Internal-Auth is the cryptographic mechanism allowing the Vitale card to authenticate itself either with symmetric crypto (online) or asymmetric crypto (offline). FCS_CKM.3 defines the access rules for the cryptographic keys. FCS_CKM.6 defines the secure deletion of the Secure Messaging Keys.
F.RATIF – Retry Counter	FMT_MTD.1/Config_Counter FIA_AFL.1	FIA_AFL.1 enforces the retry counter policy, ensuring that after a number of failed attempts, further access is blocked. FMT_MTD.1/Config_Counter defines the role that can configure the counter limit value.
F.RATIF_K_Usage – Key Usage Counter	FMT_MTD.1/Config_Counter FCS_CKM.3	FCS_CKM.3 defines the Key Usage Counter as a rule to access the keys. FMT_MTD.1/Config_Counter defines the role that can configure the counter limit value.
F.APP_INTEGRITY – Application Integrity	FPT_TST.1 FDP_UIT.1/SM FPT_FLS.1 FCS_COP.1/Seal FDP_SDI.2	FPT_TST.1 verifies system integrity, including integrity of user data. FDP_UIT.1/SM ensures data integrity during exchanges. FPT_FLS.1 maintains a secure state, and FCS_COP.1/Seal ensures integrity protection of DTBS against unauthorized alterations. FDP_SDI.2 defines the integrity rules over stored data and action in case of integrity error.

10 Technical terms, Abbreviations and References

10.1 Technical terms

Term	Definition
Administrator/Admin	User who performs TOE initialization, TOE personalization, or other TOE administrative functions
User	Entity (human user or external IT entity) outside the TOE that interacts with the TOE.
CAC	« Chaîne d'Administration de la Carte », stands for "Card Administration Chain" and is the Vitale card update portal. This update allows you to update the Vitale1 file and invalidate the Vitale card.
Data to be signed (DTBS)	Data to be signed, used as input in a single seal creation operation for the "PSO COMPUTE CRYPTOGRAPHIC CHECKSUM" command.
Secure messaging	Secure messaging using encryption and message authentication code ac-cording to ISO/IEC 7816-4.
Signatory	Legitimate *Admin* of the Vitale card who is authorized to operate the signature/seal creation.
Security Data Object (SDO)	Objects that affect either the access control policy or the implementation of the application's cryptographic processes.
Counterfeit	An unauthorized copy or reproduction of a genuine security document made by whatever means.
Embedded Software	Software embedded in an IC and not being designed by the IC developer. The IC Embedded Software is designed in the design life phase and embedded into the IC in the manufacturing life phase of the TOE.
Forgery	Fraudulent alteration of any part of the genuine document, e.g. changes to the biographical data or the portrait.
IC Dedicated Software	Software developed and injected into the chip hardware by the IC Manufacturer. Such software might support special functionality of the IC hardware and be used, amongst other, for implementing delivery procedures between different players. The usage of parts of the IC Dedicated Software might be restricted to certain life phases.
IC Identification Data	The IC Manufacturer writes a unique IC identifier to the chip during the IC manufacturing and the delivery process to the TOE manufacturer.

Term	Definition
Initialization Data	Any data defined by the TOE Manufacturer and injected into the non-volatile memory by the Integrated Circuits manufacturer during *Phase 3*. These data are for instance used for traceability and for IC identification (IC identification data).
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Manufacturer	The generic term for the IC Manufacturer producing the integrated circuit. The Manufacturer is the default user of the TOE during *Phase 3* (IC Manufacturing)
Personal Data	Data of the "End user" stored in the Vitale card according to the Logical File Structure as specified in [FSP] . It presents readable data including (but not limited to): (1) personal data of the "end user" (name, date of birth, etc.) (2) the data contained in the different EFs and SDOs.
[NIST SP 800-90]	The NIST SP 800-90A rev.1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015
Personalization Agent Key	Symmetric cryptographic authentication key used by : (1) the Personalization Agent to prove their identity and get access to the Vitale card and (2) by the Vitale card to verify the authentication attempt of the terminal as Personalization Agent according to the SFR FIA_UAU.4, FIA_UAU.5.

10.2 Abbreviations

Acronym	Definition
ADF	Application Dedicated File
$K_{IFD/ICC}$	$\mathbf{K_{IFD/ICC} = K_{IFD} \oplus K_{ICC}}$: $\mathbf{K_{IFD}}$ and $\mathbf{K_{ICC}}$ are secrets keys 32 bytes
AES	Advanced Encryption Standard
AMC	Assurance Maladie Complémentaire, stand for Supplementary Health Insurance
AMO	Assurance Maladie Obligatoire, stand for Compulsory Health Insurance
CAC	Chaine d'Administration des Cartes
CPLC	Card Production Life Cycle

Acronym	Definition
CVC	Card Verifiable Certificate
DEMA	Differential Electromagnetic Analysis
DF	Dedicated File
DO	Data Object
SDO	Secured Data Object
DPA	Differential Power Analysis
EF	Elementary File
GIE SV	Groupement d'Intérêt Economique SESAM-Vitale
ID	Identifier
INSI	IN Smart Identity
ISD	Issuer Security Domain
FSE	Feuille de Soins Electronique stand for Electronic Health Form
DRE	Demandes de Remboursement Electronique stand for Electronic Requests for Reimbursement
IC	Integrated Chip
ITSEF	Information Technology Security Evaluation Facility
MAC	Message authentication code
SAML	
SAR	Security Assurance Requirements
SE	Security Environment
SFR	Security Functional Requirements
SV	SESAM-VITALE Card
TDES	Triple Data Encryption Standard
TLSi	TéLéService Intégré

Acronym	Definition
TOE	Target Of Evaluation
TSF	TOE Security Function
EAL	Evaluation Assurance Level
TSS	TOE Summary Specification
SCV	Services de Confiance Vitale
CAP	JavaCard Converted APplet (CAP) file format

10.3 References

Reference	Description
[AGD_OPE]	FQR 151007-239- Guide d'utilisation Manuel utilisateur
[AGD_PRE]	FQR 151007-238 - Guide d'utilisation Manuel de Pré-Personnalisation – Personnalisation
[BAC PP]	*Common Criteria Protection Profile Machine Readable Travel Document with "ICAO Application", Basic Access Control* Common Criteria - Version 1.10 - March 25, 2009 Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-CC-PP-0055-2009
[CARTE-NT-010]	*Contenu de la prochaine carte Vitale, Marché MCV3* Sesam-Vitale – Version 01.00 - November 21, 2023
[CC2022]	All CC :2022 parts – [CC1], [CC2], [CC3], [CC5], [CC-ERRATA]
[CC1]	*Common Criteria for information Technology Security Evaluation, Part 1: Introduction and general model* Common Criteria - CC:2022 – Revision 1 - November 2022 Certificate reference CCMB-2022-11-001
[CC2]	*Common Criteria for information Technology Security Evaluation, Part 2: Security Functional component* Common Criteria - CC:2022 – Revision 1 - November 2022 Certificate reference CCMB-2022-11-002
[CC3]	*Common Criteria for information Technology Security Evaluation, Part 3: Security Assurance components* Common Criteria - CC:2022 – Revision 1 - November 2022 Certificate reference CCMB-2022-11-003

Reference	Description
[CC5]	*Common Criteria for information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements* Common Criteria - CC:2022 – Revision 1 - November 2022 Certificate reference CCMB-2022-11-005
[CC-ERRATA]	*Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)* Common Criteria - CC:2022 – Version 1.2 – October 15, 2025
[CEM]	*Common Methodology for Information Technology Security Evaluation -Evaluation methodology* Common Criteria - CEM:2022 – Revision 1 - November 2022 Certificate reference CCMB-2022-11-006
[CR-IC]	*Certification Report SCR 404U* ANSSI (Agence nationale de la sécurité des systèmes d'information) – Version B - February 12, 2025 Certificate reference ANSSI-CC-2023/37-R01
[CR-PL]	*Certification Report ID-One Cosmo X², version 09A111* TrustCB – Version 1 - July 11, 2025 Certificate reference NSCIB-2400104-01
[DIR]	*DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures*. European Union – December 11, 2008
[EMV_CPS1.0]	*EMV Card Personalization Specification* EMVCo – Version 1.0 – June 2003
[ECDSA]	ANSI x9.62-2005 Public Key Cryptography for the Financial Services Industry – The Elliptic Curve Digital Signature Algorithm (ECDSA)
[ESIGN K 1]	*Application Interface for smart cards used as Secure Signature Creation Devices - Part 1 - Basic requirements* Version 1 Release 9 rev2 – December 22, 2003
[FSP]	VITALE application specification: FQR 151007-236 - Spécification fonctionnelle – VITALE
[IAS-PREMIUM]	*Identification Authentication Signature (IAS) Premium - Technical Specifications* Revision: 1.0.1 - October 2006
[ISO14443]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2016

Reference	Description
[ISO7816-4]	ISO 7816 4 part 4 ISO/IEC 7816: Identification cards — Integrated circuit cards.
[ISO/IEC 9797-1]	ISO/IEC 9797-1 padding 2
[JC]	Includes [JCAPI], [JCVM] and [JCRE]
[JCAPI]	*Java Card 3.1 Classic – Application Programming Interfaces* Oracle Technology Network - Version 3.1 - 2019
[JCVM]	*Java Card Platform - Virtual Machine Specification, Classic Edition* Oracle Technology Network - Version 3.1 - November 2019
[JCRE]	*Java Card Platform - Runtime Environment Specification, Classic Edition* Oracle Technology Network - Version 3.1 - November 2019
[NIST 800-38A]	Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001
[NIST 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005
[PG-083]	RÈGLES ET RECOMMANDATIONS CONCERNANT LE CHOIX ET LE DIMENSIONNEMENT DES MÉCANISMES CRYPTOGRAPHIQUES version 3.00, 2026-03-20
[PP0084]	*Security IC Platform Protection Profile with Augmentation Packages* EUROSMART - Version 1.0 – January 13, 2014 Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-CC-PP-0084-2014.
[PP_JAVACARD]	Java Card System - Open Configuration Protection Profile, Version 3.0.5 December 2017, BSI-CC-PP-0099-2017
[PTF_AGD_OPE]	*ID-One Cosmo X² Reference Guide* IN Smart Identity - FQR 110 A334 Ed2
[RSA-PKCS#1]	PKCS#1 RSA Cryptography standards v2.2, October 27th, 2012
[ST-IC]	*SCR404U, Security Target Lite - Reference SEC222* IDEMIA - Version 1.5 – October 22, 2024
[ST-PL]	*Public Security Target ID-One Cosmo X²* IN Smart Identity - FQR 151007-243 – Revision 3 - June 30, 2025
[SV_DOC]	Cartographie des processus cryptographiques de production et exploitation de la carte Vitale – Version 0.4 – June 03, 2025

Reference	Description
[GPC_SPE_014]	GlobalPlatform Card Technology - Secure Channel Protocol '03', Card Specification v2.3 – Amendment D" Version 1.1.2 - Public Release March 2019
[FIPS_197]	FIPS 197, Federal Information Processing Standards Publication (FIPS PUB 197), Advanced Encryption Standard (AES)
[NIST_800_38B]	NIST Special Publication 800-38B: 2005, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005
[NIST SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions, November 2008

11 Index