Date: 2015-08

PP HSM CMCKG 14167-3

Protection Profiles for TSP cryptographic modules – Part 3: Cryptographic module for CSP key generation services

Module de sécurité matériel pour les services de génération de clé des prestataires de services de certification

Document type: Technical Specification
Document language: E

Contents

Page

Introduction

This CEN Technical Standard specifying a Protection Profile for Cryptographic Module for CSP Key Generation Services is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) as update of the Electronic Signatures (E-SIGN) CEN/ISSS workshop agreement (CWA) 14167-3:2004.

The document is for use by the European Commission in accordance with the procedure laid down in Article 9 of the Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [1], referred to as the 'Directive' in the remainder of the Protection Profile, as generally recognised standard for electronic-signature products in the Official Journal of the European Communities.

The Directive states in Annex II that certification-service-providers must:

(f) use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them;

(g) take measures against forgery of certificates, and, in cases where the certification-service-provider generates signature-creation data, guarantee confidentiality during the process of generating such data;

In the supporting ETSI Technical Specification "Policy Requirements for Certification Authorities (CA) issuing Qualified Certificates" (ETSI TS 101 456) [8], it is stated that the CA[1] shall ensure that:

any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured (see the Directive [1], annex II (f) and (j)).

And, if the CA generates the subject keys:

a) CA-generated subject keys shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures during the validity of the certificate;

b) CA-generated subject keys shall be of a key length and for use with a public key algorithm which is recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate;

c) CA-generated subject keys shall be generated and stored securely before delivery to the subject.

d) The subject's private key shall be delivered to the subject, if required via the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole control.

e) Once delivered to the subject any copies of the subject's private key held by the CA shall be destroyed.

This Protection Profile (PP) defines the security requirements of a Cryptographic Module (CM) used by CSP as part of its trustworthy system to provide key generation services. The Cryptographic Module, which is the Target of Evaluation (TOE), is used for the creation of subscriber private keys, and loading them into secure signature creation devices (SSCD) as part of a subscriber device provision service. Such keys are referred to in this PP as subscriber signature creation data. A cryptographic module for CSP key generation services is needed particularly to import such key into the SSCD [9].

[1] In the remainder of this PP the term "Certificate Service Provider (CSP)" is used instead of the commonly used term "Certification Authority (CA)", as the former is employed by the Directive [1] this PP aims to support.

The subscriber signature creation data generated by the TOE may be used to produce qualified electronic signatures, as defined by the Directive, or electronic signatures not necessarily qualified (e.g. advanced electronic signatures, digital signatures for other purposes different than authentication, etc.).

The TOE may implement additional functions and security requirements, e.g. for CSP Signing Operations. However, these additional functions and security requirements are not subject of this PP.

In Article 3.5, the Directive further states that

The Commission may, in accordance with the procedure laid down in Article 9, establish and publish reference numbers of generally recognised standards for electronic-signature products in the Official Journal of the European Communities. Member States shall presume that there is compliance with the requirements laid down in Annex II, point (f), and Annex III when an electronic signature product meets those standards.

This PP is established by CEN/ISSS for use by the European Commission, with reference to Annex II (f) and Annex III, in accordance with this procedure.

The document has been prepared as a Protection Profile following the rules and formats of the Common Criteria version 3.1 R3 [2] [3] [4]. This PP has been evaluated, and the corresponding Common Criteria certificate can be found in [5].

The set of algorithms and parameters for secure signature-creation devices shall be in accordance with national guidance, and subject to each Certification Body. Notwithstanding, recommendations for algorithms and parameters for secure electronic signatures are given in [6].

This document supersedes CWA 14167-3:2004.

Correspondence and comments to this Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP) should be referred to:

Editor: Dr. Jorge López Hernández-Ardieta

Email: jlhardieta@indra.es

Document Structure

Section 1 provides the scope of the Protection Profile.

Section 2 provides normative references of applicability to this Protection Profile.

Section 3 provides the terms and definitions used along the document.

Section 4 contains the Introduction of the Protection Profile, including the PP reference and the TOE overview.

Section 5 includes the conformance claims for this Protection Profile.

Section 6 contains the security problem definition, including the set of TOE assets to protect, the expected threats to those assets, the organisational security policies in place and the assumptions made on the TOE.

Section 7 contains the security objectives for the TOE and the TOE operational environment, and which address the threats, organisational security policies and assumptions considered. This section also includes a rational of correspondence between the security objectives and the threats, organisational security policies and assumptions.

Section 8 contains the security functional requirements (SFR) and security assurance requirements (SAR) derived from the Common Criteria (CC) Part 2 [3] and Part 3 [4], respectively, and that must be satisfied by the TOE and developer. This section introduces first the formalism used to describe the operations (refinement, selection, assignment and iteration) applied along the SFR descriptions. After the SFR and SAR have been described, this section provides the rationale to explicitly demonstrate that the set of SFR are complete with respect to the objectives, and that each security objective is addressed by one or more SFR. Arguments are provided for the coverage of each objective. The rational part also provides a justification for the selection of EAL4+ AVA_VAN.5 as the assurance level.

Finally, a bibliography is given.

1 Scope

This Technical Standard specifies a protection profile for cryptographic module for CSP key generation services.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.

ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.

ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.

NOTE Next documents are equivalent to the aforementioned ISO/IEC 15408 standards:

Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3. CCMB-2009-07-001, July 2009.

Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 3. CCMB-2009-07-002, July 2009.

Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 3. CCMB-2009-07-003, July 2009.

3 Terms and definitions

For the purposes of this document, the terms and definitions contained in Part 1 apply.

4 Introduction

4.1 PP reference

Title:	Cryptographic module for CSP key generation services protection profile CMCKG-PP
Author:	Jorge López Hernández-Ardieta
Version:	0.20
Publication date:	2015

4.2 TOE overview

4.2.1 TOE usage and major security features

The TOE is a Cryptographic Module (CM) used for the generation of subscribers Signature Creation Data (Subscriber-SCD) and Signature Verification Data (Subscriber-SVD) and their export to the subscribers Secure Signature Creation Devices (SSCD), in a manner that:

- The confidentiality and integrity of the Subscriber-SCD are maintained both when managed by the TOE and during transfer from the TOE to an external entity (i.e. the Subscriber-SSCD).

- The integrity of the Subscriber-SVD is maintained both when managed by the TOE and during transfer from the TOE to an external entity (i.e. the Subscriber-SSCD or the certificate generation application, CGA).

- The TOE services (generation of subscribers Subscriber-SCD/Subscriber-SVD and their export to the subscribers SSCD/CGA) are only used in an authorized way.

The TOE shall provide the following additional functions to protect the TOE services:

- User authentication.

- Access control for use of the Subscriber-SCD/SVD generation and export functions.

- Auditing of security-relevant changes to the TOE.

- Self-test of the TOE.

The TOE shall handle the following User Data:

- Subscriber Signature Creation Data (Subscriber-SCD): private key of a subscriber created internally in the TOE and loaded into a SSCD.

- Subscriber Signature Verification Data (Subscriber-SVD): public key of a subscriber created internally in the TOE and loaded into a SSCD, transferred to a CGA, or both. This data may also be distributed to additional entities.

The TOE shall, as a minimum, support the following user categories (roles):

- Crypto-officer, authorized to install, configure and maintain the TOE, and to generate and export Subscriber-SCD/SVD pairs.

- Auditor, authorized to read audit data generated by the TOE and exported for audit review in the TOE environment.

The Crypto-officer is responsible for the day-by-day operation of the TOE, including user management. The TOE should manage two or more user accounts for the role Crypto-officer to allow dual person control for security critical actions like generation and export of Subscriber-SCD/SVD pairs.

The TOE supports a separate Auditor role authorized to manage and review audit data generated by the TOE in the TOE environment. The Crypto-officer will be able to read but not to delete audit data. The Auditor shall not be able to initiate the functions to generate and/or export Subscriber-SCD/Subscriber-SVD.

The TOE may support other roles or sub-roles in addition to the roles specified above. The roles may also be allowed to perform additional functions provided by the TOE as long as the separation between different roles is given. As stated above for the auditor role, none of those additional roles shall be able to generate and/or export Subscriber-SCD/SVD pairs.

The interface to the TOE may be either shared between the different user categories, or separated for certain functions. Authentication for all user categories shall be identity-based.

Next Figure shows an overview of the TOE and its relations with the operational environment and TOE users.

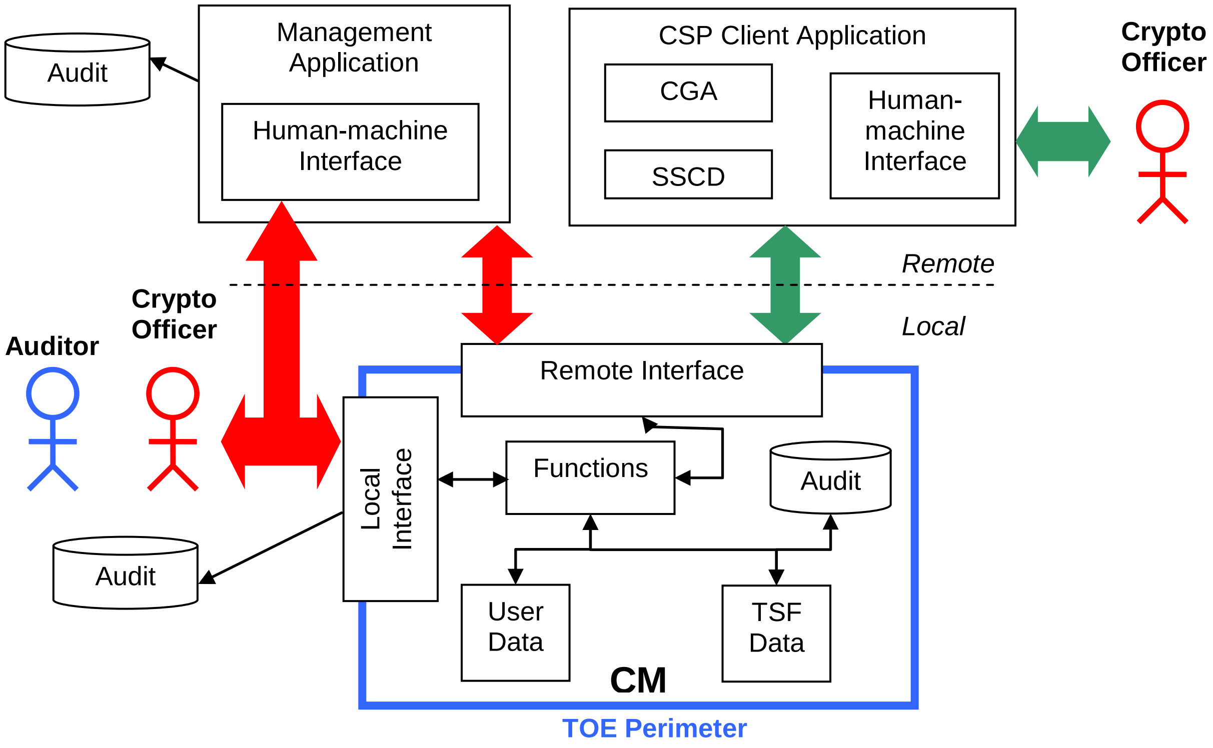

Figure 1 — TOE Overview

As can be seen in the Figure, no relation exists with Trusted Service Providers (TSP). Users can access the TOE services using local and remote interfaces. Users holding the role Crypto-officer or Auditor can access the TOE remotely, by means of the Management Application, or locally. In addition, Crypto-officers can also access the TOE in a remote manner using the CSP Client Application, which provides support to the CGA and SSCD operations.

4.2.2 TOE type

The TOE will be a separate component within the CSP boundaries with its own hardware and software, communicating via a well-defined physical and logical interface with the CSP Client Application and the Management Application. Examples of physical interfaces that may be used to connect the TOE to the CSP Client Application and Management Application are the PCI bus, the SCSI bus, USB or Firewire.

4.2.3 Available non-TOE hardware/firmware/software

None. The TOE is an independent cryptographic module comprising its own hardware, software and firmware.

5 Conformance Claims

5.1 CC conformance claim

This Protection Profile (PP) complies with Common Criteria, version 3.1, revision 3, July 2009, for both the content and presentation requirements.

All functional and assurance security requirements laid out in this PP comply with CC Part 2 and CC Part 3 respectively of the aforementioned Common Criteria version.

This PP is conforming to assurance package Evaluation Assurance Level 4 augmented (EAL4+) as defined in Part 3 of the aforementioned Common Criteria version. Augmentation results from the selection of:

- AVA_VAN.5 Advanced methodical vulnerability analysis

5.2 PP claim

This PP does not claim conformance to any other PP.

5.3 Conformance rationale

This PP does not provide a conformance rationale because it does not claim conformance to any other PP.

5.4 Conformance statement

The PP requires strict conformance of the ST or PP claiming conformance to this PP.

6 Security Problem Definition

6.1 TOE assets

The primary assets that need to be protected by the TOE are the following:

TOE services:

- **R.SERVICES**: user identity and role management, generation of Subscriber-SCD/Subscriber-SVD and their export to the subscribers SSCD, and internal audit. TOE services have to be protected in integrity and availability.

TOE internal data:

- **R.SUBSCRIBER-SCD**. Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature (defined in the Directive [1], article 2.4). Subscriber-SCD has to be protected both in confidentiality and integrity.

- **R.SUBSCRIBER-SVD**. Data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature (defined in the Directive [1], article 2.4). Subscriber-SVD has to be protected in integrity.

- **R.AUDIT_DATA**. Internal audit records and that have to be protected in integrity and availability.

- **R. TSF_DATA**: TSF data, including:

  - VAD and RAD, which have to be protected in confidentiality, integrity and availability.

  - Non-confidential user/role related data (identifier, access control lists, role definitions, etc.). These data have to be protected in integrity.

Next table correlates the TOE internal data types explained above with those data types considered in the formalisation of the security functional requirements (SFR):

TOE internal data type	SFR-related data type
R.SUBSCRIBER-SCD	User data[1]
R.SUBSCRIBER-SVD	
R.AUDIT_DATA	
R. TSF_DATA	TSF data[2]

[1] data for the user that does not affect the operation of the TSF (TOE Security Functionality). For example, in the case of R.AUDIT_DATA, the audit records generated internally in the TOE are intended to be revised by the Auditor.

[2] data for the operation of the TOE upon which the enforcement of the SFR relies.

6.2 Threats

The expected attackers are qualified so as to have high attack potential, in accordance with the security assurance given by AVA_VAN.5 Advanced methodical vulnerability analysis.

The expected threat agents are:

- **TA.EXTERNAL**

  This agent represents an entity that does not hold any authorised role to operate or interact with the TOE. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE. Examples of this threat agent are: unauthorised CSP personnel, cybercriminals, and hackers in general.

- **TA.INSIDER**

  This agent represents an entity that holds an authorised role to operate or interact with the TOE, and which has the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE. Examples of this threat agent are: auditors and crypto-officers.

- **TA.INADVERTENT**

  This agent represents an entity that holds an authorised role to operate or interact with the TOE, but which does not have the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE. Examples of this threat agent are: auditors and crypto-officers.

The expected threats to the TOE may be:

- **T.Bad_SW** Malicious Software during the Lifetime of the TOE

  A TA.EXTERNAL or a TA.INSIDER might try to load malicious software into the TOE in order to modify or gain illicit access to R.SUBSCRIBER-SCD, R.AUDIT_DATA, R.TSF_DATA or R.SERVICES.

  For example, a TA.EXTERNAL, using the TOE remote interface, may inject a malicious code (malware) into the TOE. Later on, this malware may compromise the confidentiality of the R.SUBSCRIBER-SCD by exfiltrating its value from the TOE boundaries.

- **T.Insecure_Init** Insecure Initialisation of the TOE

  A TA.EXTERNAL, a TA.INSIDER or a TA.INADVERTENT may initialise the TOE with insecure R.TSF_DATA.

- **T.Malfunction** Malfunction of TOE

  There is no active agent for this threat.

  An internal malfunction of TOE functions may result in:

  - misuse of R.SERVICES,
  - disclosure or alteration of R.SUBSCRIBER-SCD,
  - alteration of R.SUBSCRIBER-SVD,
  - denial of R.SERVICES for authorised users,
  - alteration of R.AUDIT_DATA or R.TSF_DATA.

  This includes the destruction of the TOE as well as hardware failures, which prevent the TOE from performing its services.

  This includes also the destruction of the TOE by environmental failure.

Finally, this includes some kind of physical tampering that induces erroneous behaviour from the underlying hardware or software of the ToE.

Technical failure may result in an insecure operational state violating the integrity and availability of the TOE services.

The correct operation of the TOE also depends on the correct operation of critical hardware components. Critical components might be:

- the central processing unit
- a coprocessor for accelerating cryptographic operations
- a physical random number generator
- storage devices used to temporarily store cryptographic keys
- physical I/O device drivers

– **T.Misuse** Misuse of TOE

A TA.INSIDER or a TA.INADVERTENT, who has access to the TOE R.SERVICES, uses these services in a manner for which they are not intended to, or without proper authorisation, having an impact on the R.SUBSCRIBER-SCD, R.SUBSCRIBER-SVD, R.AUDIT_DATA or R.TSF_DATA.

For instance, a TA.INSIDER such as CSP personnel without authorisation to generate R.SUBSCRIBER-SCD and R.SUBSCRIBER-SVD pairs may misuse the TOE R.SERVICES to do so.

– **T.Phys_Manipul** Physical Manipulation of the TOE

A TA.EXTERNAL or a TA.INSIDER may try to physically manipulate the TOE with the intent to derive all or part of the R.SUBSCRIBER-SCD (by side channel for example), to misuse TOE R.SERVICES, or alter R.TSF_DATA or R.AUDIT_DATA. This threat also includes the destruction of the TOE by deliberate action.

– **T.Subscriber-SCD_Alteration** Alteration of the Subscriber-SCD

A TA.EXTERNAL or a TA.INSIDER might modify or alter the R.SUBSCRIBER-SCD while being operated inside the TOE or during transfer to the SSCD, resulting in a loss of integrity of the R.SUBSCRIBER-SCD.

– **T.Subscriber-SCD_Copy** Uniqueness of Subscriber-SCD

A TA.EXTERNAL, a TA.INSIDER or a TA.INADVERTENT may cause that a R.SUBSCRIBER-SCD generated by the TOE is transferred to more than one SSCD, resulting in the possibility for one owner of such a SSCD to forge the signature of the owner of another SSCD that uses the same SCD.

– **T.Subscriber-SCD_Derive** Deriving All or Parts of Subscriber-SCD

A TA.EXTERNAL or a TA.INSIDER might derive all or parts of R.SUBSCRIBER-SCD in any way. This includes using knowledge about the key generation process, even during legitimate use of the R.SERVICES.

– **T.Subscriber-SCD_Disclose** Disclosing All or Part of Subscriber-SCD

A TA.EXTERNAL or a TA.INSIDER might disclose all or part of R.SUBSCRIBER_SCD over physical or logical TOE interface by bypassing the export control mechanisms.

– **T.Subscriber-SVD_Alteration** Alteration of the Subscriber-SVD

A TA.EXTERNAL or a TA.INSIDER might modify or alter the R.SUBSCRIBER-SVD exported by the TOE to the CGA or the Subscriber-SSCD, resulting in a loss of integrity of the R.SUBSCRIBER-SVD.

6.3 Organisational security policies

- **P.Algorithms** Use of Approved Algorithms and Algorithm Parameter

  Only approved algorithms and algorithm parameters defined as acceptable for being used in R.SUBSCRIBER-SCD/R.SUBSCRIBER-SVD pair generation for secure electronic signatures shall be used by the TOE. This includes the generation of random numbers and the quality of the R.SUBSCRIBER-SCD/R.SUBSCRIBER-SVD pairs generated.

  Approved algorithms and algorithm parameters defined as acceptable shall be used to ensure the confidentiality and integrity of R.SUBSCRIBER-SCD, and the integrity of R.SUBSCRIBER-SVD.

  The TOE shall support cryptographic algorithms and key lengths conformant to the rules defined by the relevant national CC Certification Body.

Note: A list of proposed algorithms and parameters for use across Europe is given in [6].

Application note: The PP/ST writer should ensure that the algorithms and algorithms parameters specified in the PP/ST conform to the rules and recommendations defined by the national authority.

6.4 Assumptions

- **A.Audit_Support** CSP audit review

  The CSP reviews the audit trail generated and exported by the TOE. The client application receives and stores the audit trail of the TOE for review by the System Auditor of the CSP (Role Auditor) according to the audit procedure of the CSP.

- **A.Secure_Channel** Interface with Human Users

  The CSP Client Application and the Management Application will provide an appropriate human-machine interface and communication path between human users and the TOE for remote authentication and management services. The TOE environment transmits identification, authentication and management data of TOE users to the TOE in a manner that the integrity and confidentiality of data are assured.

- **A.Trusted_Environment** Trustworthiness of operating personnel and physical security

  The cryptographic module operates in a secure environment with policy for trustworthiness of operating personnel and physical security of the environment.

7 Security Objectives

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent to counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

7.1 Security objectives for the TOE

- **O.Attack_Response** Response to Physical Attacks

  The TOE shall detect attempts of physical tampering and, in such cases, securely delete any R.SUBSCRIBER-SCD if this data has not already been deleted.

- **O.Audit** Generation and Export of Audit Data

  The TOE shall audit the following events:

  - TOE initialisation
  - TOE start-up
  - Generation of R.SUBSCRIBER-SCD/ R.SUBSCRIBER-SVD pairs
  - Export of R.SUBSCRIBER-SCD/ R.SUBSCRIBER-SVD pairs
  - Destruction of R.SUBSCRIBER-SCD/ R.SUBSCRIBER-SVD pairs
  - Unsuccessful authentication
  - Modification of TOE user management data
  - Adding new users or roles
  - Deleting users or roles
  - Unsuccessful self test operations
  - Execution of the TSF self tests during initial start-up, installation, maintenance, and at the request of the authorised user
  - Exporting and deleting audit trail records
  - Unsuccessful restore attempt
  - Software modification
  - Tamper detection event

  The audit data shall associate each auditable event with the identity of the user that caused the event. The integrity of the audit trail shall be ensured. The TOE shall export the audit data upon request of the Auditor and the Crypto-officer. The TOE shall provide the management function for the audit to the Auditor only.

- **O.Check_Operation** Check for Correct Operation

  The TOE shall perform regular checks to verify that its components operate correctly. This includes integrity checks and/or authenticity of TOE software, firmware, internal TSF data or user data during initial start-up, at the request of the authorised user, randomly during the critical steps of cryptographic process, and during installation, maintenance and update processes.

- **O.RBAC** Rol-based Access Control to TOE Services

  The TOE shall restrict the access to its assets (TOE services and TOE internal data) depending on the user role, allowing user access only to those services and data explicitly authorised to the assigned role. Assignment of services to roles shall be done either by explicit action of a Crypto-officer or by default. Roles may also be predefined in the production or initialisation phase.

- **O.Secure_State** Secure State in Case an Error is Detected

  The TOE shall enter a secure state whenever it detects a failure or an integrity error of software, firmware, internal TSF data or user data. The secure state shall prevent the loss of confidentiality of any R.SUBSCRIBER-SCD.

- **O.Subscriber-SCD/SVD_Generation** Subscriber-SCD/SVD Pair Generation

  For the R.SUBSCRIBER-SCD/ R.SUBSCRIBER-SVD pair generation, the TOE shall implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority. The TOE implementation shall also be resistant against state-of-the-art side channel attacks that may compromise the confidentiality of the R.SUBSCRIBER-SCD.

- **O.Subscriber-SCD_Management** Secure Management of Subscriber-SCD

  The TOE shall ensure the confidentiality and integrity of the R.SUBSCRIBER-SCD both when it is under the control of the TOE and during transfer from the TOE to the Subscriber-SSCD. This includes protection against disclosing completely or partly the R.SUBSCRIBER-SCD in clear through any physical or logical TOE interface. Therefore, the implementation of the TOE shall be resistant against state-of-the-art side channel attacks that may compromise the confidentiality of the R.SUBSCRIBER-SCD. The TOE shall not use any R.SUBSCRIBER-SCD for signature creation, and the R.SUBSCRIBER-SCD shall be securely deleted from the TOE whenever it is exported. For confidentiality and integrity purposes, the TOE shall also implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority.

- **O.Subscriber-SVD_Management** Secure Management of Subscriber-SVD

  The TOE shall ensure the integrity of the R.SUBSCRIBER-SVD both when it is under the control of the TOE and during transfer from the TOE to the CGA or the Subscriber-SSCD. For integrity purposes, the TOE shall also implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority

- **O.User_Authentication** Authentication of TOE Users

  The TOE shall be able to identify and authenticate the users acting with a defined role, before allowing any access to TOE protected assets (TOE services and TOE internal data). Identification and authentication shall be based on user identity.

7.2 Security objectives for the operational environment

The following security objectives relate to the TOE environment. This includes the CSP Client Application, the Management Application as well as the procedures for the secure operation of the TOE.

- **OE.Protect_Access** Prevention of Unauthorised Physical Access

  The TOE shall be protected by physical, logical and organisational protection measures implemented by the TOE environment in order to prevent any TOE modification, as well as any protected assets disclosure. Those measures shall restrict the TOE usage to authorised persons only. The TOE operational environment shall follow the policy requirements established in ETSI TS 101 456 [8].

- **OE.Audit** Audit review

  The environment shall provide a review of the audit trail recorded by the TOE. Additionally, the environment shall audit the following events:

  - Unsuccessful authentication when the Management Application or the CSP Client Application are used
  - Modification of TOE user management data when the Management Application is used
  - Adding new users or roles when the Management Application is used
  - Deleting users or roles when the Management Application is used
  - Execution of the TSF self tests during at the request of the authorised user when the Management Application is used
  - Exporting audit trail records when the Management Application is used
  - Unsuccessful restore attempt when the Management Application is used
  - Software modification when the Management Application is used

- **OE.Personnel** Reliable Personnel

  The personnel using the TOE services shall be aware of civil, financial and legal responsibilities, as well as the obligations they have to face, depending on their role. The personnel shall be trained on correct usage of the TOE.

- **OE.Secure_Channel** Reliable Human-Machine Interface

  If the CSP Client Application and the Management Application provide a human-machine interface and a communication path between human users and the TOE, these applications shall ensure the confidentiality and integrity of the data transferred between the TOE and the human user.

- **OE.Secure_Init** Secure Initialisation Procedures

  Procedures and controls in the TOE environment shall be defined and applied to permit the secure set-up and initialisation of the TOE services within a CSP system in compliance with the requirements of the EU directive and the Policy for certification authorities issuing qualified certificates [8]. This includes the initial configuration of R. TSF_DATA.

- **OE.Secure_Oper** Secure Operating Procedures

  Procedures and controls in the TOE environment shall be defined and applied to permit the secure operation of the TOE services within a CSP system in compliance with the requirements of the EU Directive and the Policy for certification authorities issuing qualified certificates [8].

- **OE.Subscriber-SCD_Management** Secure Management of Subscriber-SCD

  The Subscriber-SSCD shall ensure the confidentiality and integrity of the R.SUBSCRIBER-SCD both during transfer from the TOE and once it is under its control.

- **OE.Subscriber-SVD_Management** Secure Management of Subscriber-SVD

The CGA and the Subscriber-SSCD shall ensure the integrity of the R.SUBSCRIBER-SVD both during transfer from the TOE and once it is under their control.

7.3 Security objectives rationale

The following table shows the correspondence between the security objectives applicable to the TOE and the environment and the countered threats, the assumptions and the organizational security policies.

	T.Bad_SW	T.Insecure_Init	T.Malfunction	T.Misuse	T.Phys_Manipul	T.Subscriber-SCD_Alteration	T.Subscriber-SCD_Copy	T.Subscriber-SCD_Derive	T.Subscriber-SCD_Disclose	T.Subscriber-SVD_Alteration	P.Algorithms	A.Audit_Support	A.Secure_Channel	A.Trusted_Environment
O.Attack_Response					X									
O.Audit	X	X	X	X	X									
O.Check_Operation	X		X		X									
O.RBAC	X	X		X										
O.Secure_State	X		X		X									
O.Subscriber-SCD/SVD_Generation								X			X			
O.Subscriber-SCD_Management						X	X		X		X			
O.Subscriber-SVD_Management										X	X			
O.User_Authentication	X	X		X										
OE.Protect_Access	X	X			X									X
OE.Audit	X	X	X	X	X							X		
OE.Personnel	X	X		X								X		X
OE.Secure_Channel	X	X		X									X	
OE.Secure_Init		X						X	X					X
OE.Secure_Oper				X				X	X					X
OE.Subscriber-						X	X		X					

	T.Bad_SW	T.Insecure_Init	T.Malfunction	T.Misuse	T.Phys_Manipul	T.Subscriber-SCD_Alteration	T.Subscriber-SCD_Copy	T.Subscriber-SCD_Derive	T.Subscriber-SCD_Disclose	T.Subscriber-SVD_Alteration	P.Algorithms	A.Audit_Support	A.Secure_Channel	A.Trusted_Environment
SCD_Management														
OE.Subscriber-SVD_Management										X				

Table 1 — Mapping between Security Problem Definition and Security Objectives

Security objectives coverage is met as each threat, assumption and organizational security policy is addressed by at least one security objective, and every security objective is mapped with at least one threat, assumption or organizational security policy.

Next, the rationale for each matching is provided:

T.Bad_SW (Malicious Software during the Lifetime of the TOE) is a threat by which a TA.EXTERNAL or a TA.INSIDER might try to load malicious software into the TOE in order to modify or gain illicit access to R.SUBSCRIBER-SCD, R.TSF_DATA or R.SERVICES. This threat is countered by nine security objectives, five for the TOE, and four for the TOE operational environment. First, **O.Audit** (Generation and Export of Audit Data) ensures that operations related to the TOE initialisation, start-up and software modification – that is, operations by which malicious software could be loaded into the TOE – are audited. These audit trails can be reviewed by the authorised user due to **OE.Audit** (Audit review). Also, only users holding Crypto-Officer role can perform software/firmware update (**O.RBAC** (Rol-based Access Control to TOE Services)). Therefore a reliable authentication shall be done to ensure that user's identity (**O.User_Authentication** (Authentication of TOE Users)) is associated with the Crypto-Officer role. This authentication is supported by the secure channel provided by the environment (**OE.Secure_Channel (**Reliable Human-Machine Interface)). This security objective for the environment also ensures that the data uploaded to the ToE by the Crypto-Officer is protected in confidentiality and integrity during transfer, lowering the risk of distant software attack via the communication port of the TOE. In addition, **OE.Personnel (**Reliable Personnel) indicates that the Crypto-Officer shall be aware of civil, financial and legal responsibilities, as well as the obligations they have to face, and shall be trained on correct usage of the TOE. Thus, this security objective lowers the risk of Crypto-Officer's misbehaviour. On the other hand, **O.Check_Operation** (Check for Correct Operation) ensures that the TOE performs regular checks to verify that its components operate correctly, including integrity checks and authenticity of software/firmware. This prevents that malicious software that affects the correct operation of the TOE runs undetected. **O.Secure_State** (Secure State in Case an Error is Detected) ensures that the TOE enters a secure state whenever it detects a failure or an integrity error of software, firmware, internal TSF data or user data, preventing the loss of confidentiality of any Subscriber-SCD. Finally, **OE.Protect_Access** (Prevention of Unauthorised Physical Access) prevents any TOE modification by physical, logical and organisational protection measures implemented by the TOE environment.

T.Insecure_Init (Insecure Initialisation of the TOE) handles a threat where a TA.EXTERNAL, a TA.INSIDER or a TA.INADVERTENT may initialise the TOE with insecure R.TSF_DATA. This threat is countered by seven security objectives, three for the TOE and four for the TOE operational environment. By **O.Audit** (Generation and Export of Audit Data), the TOE shall audit the TOE initialisation, TOE start up process, modification of TOE management data and the handling of (new) users or roles which are part of the initialization process. These audit trails can be reviewed by the authorised user due to **OE.Audit** (Audit review). **O.RBAC** (Rol-based Access Control to TOE Services) ensures the assignment of services to roles either done by explicit action of a system administrator or by default and ensures that the roles may be predefined in the production or initialisation phase. In addition, and before granting access to TOE services, the authentication of users (**O.User_Authentication** (Authentication of TOE Users) and **OE.Secure_Channel (**Reliable Human-Machine Interface) to support secure transfer of credentials) is mandatory before any action is taken on the TOE assets. **OE.Personnel** (Reliable Personnel) establishes that the personnel using the TOE services shall be aware of civil, financial and legal responsibilities, as well as the obligations they have to face, depending on their role. This objective clearly acts as a deterrence measure. **OE.Protect_Access** (Prevention of Unauthorised Physical Access) restricts the TOE usage to authorised persons only, preventing any TOE modification of any protected asset. Therefore, the possibility that an attacker physically accesses the TOE to establish an insecure configuration is minimized. Finally, **OE.Secure_Init** (Secure Initialisation Procedures) deals with the procedures and controls to define and apply in the TOE environment in order to permit the secure set-up and initialisation of the TOE services.

T.Malfunction (Malfunction of TOE) represents a threat by which an incorrect operation of the TOE functions, caused by an internal malfunction, may violate several security properties of the TOE assets. This threat is countered by three security objectives for the TOE. In particular, **O.Check_Operation** (Check for Correct Operation) ensures that the TOE performs regular checks to verify that its components operate correctly, while **O.Audit** (Audit record generation and export) ensures audit information about unsuccessful self test operations detecting TOE internal errors. These audit trails can be reviewed by the authorised user due to **OE.Audit** (Audit review). Finally, **O.Secure_State** (Secure State in Case an Error is Detected) ensures that the TOE enters a secure state whenever it detects a failure or an integrity error of software, firmware, internal TSF data or user data, preventing the loss of confidentiality of any R.SUBSCRIBER-SCD. The combination of these security objectives ensures that either the TOE operates under verified secure conditions, or in case that it does not or the checks fail, the TOE enters in a secure state.

T.Misuse (Misuse of TOE) is a threat by which a TA.INSIDER or a TA.INADVERTENT may misuse the TOE R.SERVICES to forge R.SUBSCRIBER-SCD, R.SUBSCRIBER-SVD or R.TSF_DATA. This threat is countered by seven security objectives, three for the TOE and four for the TOE operational environment. By **O.Audit** (Generation and Export of Audit Data) and **OE.Audit** (Audit review) the TOE audits the modification of management of TOE TSF and user data as well as other operations carried out during TOE operation and maintenance, and these audit trails can be further reviewed by an authorised user. Thereby, any modification on these parameters is audited and can be detected by the Crypto-officer and Auditor. **O.RBAC** (Rol-based Access Control to TOE Services) ensures the assignment of services to roles either done by explicit action of a system administrator or by default and ensures that the roles may be predefined in the production or initialisation phase. In addition, and before granting access to TOE services, the authentication of users (**O.User_Authentication** (Authentication of TOE Users) and **OE.Secure_Channel (**Reliable Human-Machine Interface) to support secure transfer of credentials) is mandatory before any action is taken on the TOE assets. **OE.Personnel** (Reliable Personnel) establishes that the personnel using the TOE services shall be aware of civil, financial and legal responsibilities, as well as the obligations they have to face, depending on their role. This objective clearly acts as a deterrence measure. Finally, **OE.Secure_Oper** (Secure Operating Procedures) deals with the procedures and controls to define and apply in the TOE environment in order to permit the secure operation of the TOE services.

T.Phys_Manipul (Physical Manipulation of the TOE) deals with a TA.EXTERNAL or a TA.INSIDER which may try to physically manipulate the TOE with the intent to derive all or part of the R.SUBSCRIBER-SCD (by side channel for example), to misuse TOE R.SERVICES, or alter R.TSF_DATA or R.AUDIT_DATA. This threat is countered by six security objectives, four for the TOE and two for the TOE operational environment. The TOE shall prevent this tampering by detecting physical manipulation by entering a secure state (**O.Secure_State** (Secure State in Case an Error is Detected)) or even destroy R.SUBSCRIBER-SCD (**O.Attack_Response** (Response to Physical Attacks)). Physical manipulation can also be detected by a loss of integrity of critical data, and thus they need to be regularly checked (**O.Check_Operation** (Check for Correct Operation)). To prevent physical manipulation, the TOE shall be placed in a secure place (**O.Protect_Access** (Prevention of Unauthorised Physical Access)) and every physical manipulation shall be logged (**O.Audit** (Generation and Export of Audit Data) and **OE.Audit** (Audit review)).

T.Subscriber-SCD_Alteration (Alteration of the Subscriber-SCD) addresses a threat, represented by a TA.EXTERNAL or a TA.INSIDER, which modifies or alters the R.SUBSCRIBER-SCD while being operated inside the TOE or during transfer to the SSCD, resulting in a loss of integrity of the R.SUBSCRIBER-SCD. This threat is countered by two security objectives, one for the TOE and one for the TOE operational environment. Both security objectives, **O.Subscriber-SCD_Management** (Secure Management of Subscriber-SCD) and **OE.Subscriber-SCD_Management** (Secure Management of Subscriber-SCD), ensure the integrity of the Subscriber-SCD during its entire life-cycle, covering the time under the control of the TOE (both within its boundaries and when transmitted to the Subscriber-SSCD) and the SSCD (both within its boundaries and when transmitted from the TOE), respectively.

T.Subscriber-SCD_Copy (Uniqueness of Subscriber-SCD) deals with a threat, represented by a TA.EXTERNAL, a TA.INSIDER or a TA.INADVERTENT, by which a R.SUBSCRIBER-SCD is exported to more than one Subscriber-SSCD, permitting an attacker to masquerade as another subscriber. This threat is countered by two security objectives, one for the TOE and one for the TOE operational environment. In particular, the confidentiality of the R.SUBSCRIBER-SCD is protected during transfer from the TOE to the Subscriber-SSCD by means of **O.Subscriber-SCD_Management** (Secure Management of Subscriber-SCD) and **OE.Subscriber-SCD_Management** (Secure Management of Subscriber-SCD). As O.Subscriber-SCD_Management also establishes that the Subscriber-SCD is securely deleted from the TOE whenever it is exported, it is not possible for an attacker to re-use it for second or subsequent exports.

T.Subscriber-SCD_Derive (Deriving All or Parts of Subscriber-SCD) poses a threat, represented by a TA.EXTERNAL or a TA.INSIDER, by which the R.SUBSCRIBER-SCD generated by the TOE may be partially or totally derived by an attacker, including during legitimate use of the TOE R.SERVICES. This threat is countered by three security objectives, one for the TOE and two for the TOE operational environment. In the first place, **O.Subscriber-SCD/SVD_Generation** (Subscriber-SCD/SVD Pair Generation) establishes the need to use secure cryptographic algorithms and parameters for the R.SUBSCRIBER-SCD/ R.SUBSCRIBER-SVD pair generation, preventing the attacker to derive the cryptographic keys using cryptanalytic or brute force attacks. Secondly, a correct and secure initialization (**OE.Secure_Init** (Secure Initialisation Procedures)) and operation (**OE.Secure_Oper** (Secure Operating Procedures)) of the TOE by means of adequate procedures and controls implemented in the TOE environment ensure that the TOE uses the established configuration, including the aforementioned secure cryptographic algorithms and parameters.

T.Subscriber-SCD_Disclose (Disclosing All or Part of Subscriber-SCD) represents a threat, represented by a TA.EXTERNAL or a TA.INSIDER, by which the R.SUBSCRIBER_SCD generated by the TOE is disclosed partially or totally over any physical or logical TOE interface by a bypass of the export control mechanisms. This threat is countered by four security objectives, one for the TOE and three for the TOE operational environment. **O.Subscriber-SCD_Management** (Secure Management of Subscriber-SCD) protects the confidentiality of the Subscriber-SCD both when it is under the control of the TOE and during transfer from the TOE to the R.SUBSCRIBER_SCD, preventing an attacker to gain access to the plain text or obtain the R.SUBSCRIBER_SCD by means of a side-channel attack. Also, this security objective establishes that the R.SUBSCRIBER_SCD has to be securely deleted from the TOE whenever it is exported to the Subscriber-SSCD, undermining the possibility of a further compromise. Procedures and controls implemented in the TOE environment and applied during set-up and initialization (**OE.Secure_Init** (Secure Initialisation Procedures)) and operation (**OE.Secure_Oper** (Secure Operating Procedures)) ensure that the TOE uses the established secure configuration, and thus the secure management of the R.SUBSCRIBER_SCD is enforced. Finally, **OE.Subscriber-SCD_Management** (Secure Management of Subscriber-SCD) imposes the Subscriber-SSCD to guarantee the confidentiality of the R.SUBSCRIBER_SCD during the import from the TOE and once it is under its control. Consequently, these security objectives counter the threat at every stage of the R.SUBSCRIBER_SCD life cycle, when managed by the TOE itself, transferred to third entities, as well as under their external control.

T.Subscriber-SVD_Alteration (Alteration of the Subscriber-SVD) addresses a threat, represented by a TA.EXTERNAL or a TA.INSIDER, which modifies or alters the R.SUBSCRIBER-SVD exported by the TOE to the CGA or the Subscriber-SSCD, resulting in a loss of integrity of the R.SUBSCRIBER-SVD. This threat is countered by two security objectives, one for the TOE and one for the TOE operational environment. Both security objectives, **O.Subscriber-SVD_Management** (Secure Management of Subscriber-SVD) and **OE.Subscriber-SVD_Management** (Secure Management of Subscriber-SVD), ensure the integrity of the Subscriber-SVD during its entire life-cycle, covering the time under the control of the TOE (both within its boundaries and when transmitted to the CGA or the Subscriber-SSCD) and the CGA/Subscriber-SSCD (both within its boundaries and when transmitted from the TOE), respectively.

P.Algorithms (Use of Approved Algorithms and Algorithm Parameter) addresses the need to use only algorithms and algorithm parameter defined as acceptable by the national authority for being used for Subscriber-SCD/SVD pair generation and for ensuring the confidentiality of Subscriber-SCD and the integrity of Subscriber-SCD and Subscriber-SVD. This organizational security policy is addressed by several objectives for which it is required that the TOE uses cryptographic algorithms and parameters compliant with the requirements established by the national authority: **O.Subscriber-SCD/SVD_Generation** (Subscriber-SCD/SVD Pair Generation), which deals with the R.SUBSCRIBER-SCD/ R.SUBSCRIBER-SVD pair generation; **O.Subscriber-SCD_Management** (Secure Management of Subscriber-SCD), that deals with the operational aspects of protecting the confidentiality and integrity of the Subscriber-SCD; and **O.Subscriber-SVD_Management** (Secure Management of Subscriber-SVD), that deals with the operational aspects of protecting the integrity of the Subscriber-SVD.

A.Audit_Support (CSP audit review) is an assumption about the CSP reviewing the audit trail generated and exported by the TOE which is directly fulfilled by **OE.Audit** (Audit review), as the environment provides a review of the audit trail recorded by the TOE. **OE.Personnel** (Reliable Personnel) enhances the fulfillment of this necessity as the personnel using the TOE services shall be aware of civil, financial and legal responsibilities, as well as the obligations they have to face, depending on their role.

A.Secure_Channel (Interface with Human Users) addresses the assumption that the client application will provide an appropriate human-machine interface and communication path between human users and the TOE for remote authentication and management services. This assumption is met by **OE.Secure_Channel** (Reliable Human-Machine Interface), which indicates that the client application will ensure the confidentiality and integrity of the data transferred between the TOE and the human user.

A.Trusted_Environment (Trustworthiness of operating personnel and physical security) indicates that the cryptographic module operates in a secure environment with policy for trustworthiness of operating personnel and physical security of the environment. This assumption is met by a security objective for the personnel operating the TOE (**OE.Personnel (**Reliable Personnel)), and security objectives for the operational environment, both for the initialization of the TOE (**OE.Secure_Init (**Secure Initialisation Procedures)), and during the normal operation (**OE.Secure_Oper (**Secure Operating Procedures)). In addition to this, **OE.Protect_Access (**Prevention of Unauthorised Physical Access), ensures that the physical access to the TOE is protected by physical, logical and organisational protection measures implemented by the TOE environment.

8 Security Requirements

8.1 Security functional requirements

8.1.1 Subjects, objects, security attributes and operations

This section defines some concepts used during the definition of the security functional requirements.

Subjects:

- User of the TOE. Any user that holds an authorised role (crypto-officer, auditor) to access the services available in the TOE.

Objects and security attributes:

- Subscriber-SCD. See section 3 Terms and definitions.
- Subscriber-SVD. See section 3 Terms and definitions.
- Audit data. Internal audit records generated by the TOE during the operation.
- User’s identity. Set of data that uniquely describes and identifies a user of the TOE.
- Role. Set of permissions granted to a user of the TOE to perform certain operations on the TOE.
- TSF data related to users and roles. Information about the TOE Security Functionality (TSF), but restricted to users and roles. This includes users’ RAD (see section 3 Terms and definitions), identifier and assigned roles, the access control lists and role definitions, as well as any other information used by the TOE to authenticate users and grant accesses.

Operations:

- Generate Subscriber-SCD/Subscriber-SVD pair. Operation by which a user of the TOE uses the TOE to generate a key pair for its later export into a Subscriber-SSCD.
- Export (transmit) Subscriber-SCD/Subscriber-SVD. Operation by which a user of the TOE uses the TOE to export the key pair from the TOE into the Subscriber-SSCD.
- Export (transmit) audit data. Operation by which a user of the TOE uses the TOE to export audit data from the TOE to the TOE environment.
- Delete audit data. Operation by which a user of the TOE uses the TOE to delete audit data.
- Query one’s own RAD, users’ identity, roles and binding between users and roles. Operation by which a user of the TOE uses the TOE to access to certain information related to the users, including its own RAD (see section 3 Terms and definitions), the identity of users of the TOE, the existing roles, and the roles assigned to the users of the TOE.
- Modify one’s own RAD, users’ identity, roles and binding between users and roles. Operation by which a user of the TOE uses the TOE to access to and modify certain information related to the users, including its own RAD (see section 3 Terms and definitions), the identity of users of the TOE, the existing roles, and the roles assigned to the users of the TOE.
- Delete users’ identity, roles and binding between users and roles. Operation by which a user of the TOE uses the TOE to delete certain information related to the users, including its own RAD (see section 3 Terms and definitions), the identity of users of the TOE, the existing roles, and the roles assigned to the users of the TOE.

8.1.2 Security requirements operations

Common Criteria allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Part 1 of CC. Each of these operations is used in this PP as follows:

- A refinement operation is used to add detail to a requirement, and thus further restricts a requirement. A refinement of a security requirement is included in text as *italicized and underlined* text. In cases where words from a CC requirement were deleted, the deleted text appears ~~crossed out~~.

- A selection operation is used to select one or more options provided by the CC in stating a requirement. A selection is indicated in square brackets with selected option as underlined text, italicized and in blue colour [selection: *minimum*]. Selections left to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, and with the available options italicized and in blue colour [selection*: minimum, basic, detailed, not specified*].

- An assignment operation is used to assign a specific value to an unspecified parameter. An assignment is indicated in square brackets with the specific value as underlined text, italicized and in blue colour [assignment: *none*]. Assignments left to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made, and with the original text italicized and in blue colour [assignment: *other audit relevant information*].

- An iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash “/", and the iteration indicator after the component identifier.

8.1.3 Security Audit (FAU)

FAU_GEN.1 Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

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

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

b) All auditable events for the [selection: *minimum*] level of audit; and

c) [assignment:

- *Start-up and initialization of the TOE.*
- *Shut down of the TOE.*
- *Software update, modification or installation, if supported by the TOE.*
- *Initialization and finalization of a user session.*
- *Attempts of initiating a user session.*
- *Changes of privileges assigned to any role.*
- *Access to the security attributes of the TOE.*
- *Unsuccessful attempts to access the TOE resources.*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *none*].

FAU_GEN.2 User identity association

Dependencies: FAU_GEN.1 Audit data generation

FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_STG.2 Guarantees of audit data availability

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [selection: *prevent*] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records that have not been exported by the auditor*] stored audit records will be maintained when the following conditions occur: [selection: *audit storage exhaustion*]

Application note: The TSF may overwrite the audit trail data after reading (export) by the Auditor. The ST writer shall perform the assignment for the metric for saving audit records according the storage provided for audit events. This metric should implement security mechanisms to ensure availability of audit data in case of audit storage exhaustion because of limited storage of audit events. For example, if the storage is exhausted, the TOE would

(i) stop the normal operation,

(ii) inform the actual user about exhaustion of the audit event storage and

(iii) continue the normal operation only after export and deletion of audit data.

8.1.4 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. *The standards shall be selected from the list of approved algorithms and parameters, in accordance with national guidance, and subject to each Certification Body. Notwithstanding, recommendations for algorithms and parameters for secure electronic signatures are given in [6].*

Application note: FCS_CKM.1 describes the generation of the Subscriber-SCD/SVC pair. The ST writer shall specify the algorithm applied for generating random numbers that are used to generate the Subscriber-SCD/SVD pair.

Application note: The ST writer should iterate FCS_CKM.1 if the TOE generates cryptographic keys used by TSF for the transfer of other user data over a trusted channel (FTP_ITC.1) or trusted path (FTP_TRP.1).

FCS_CKM.4 Cryptographic key destruction

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

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

Application note: FCS_CKM.4 describes the secure deletion of the Subscriber-SCD immediately after the TSF has exported the Subscriber-SCD. The TSF shall destroy the Subscriber-SCD and all other plaintext secret or private keys, if the TSF required by FPT_PHP.2 detects physical tampering.

Application note: The ST writer should iterate FCS_CKM.4 if the TOE generated cryptographic keys used by TSF for the transfer of other user data over a trusted channel according (FTP_ITC.1) or trusted path (FTP_TRP.1).

FCS_COP.1 Cryptographic operation

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [assignment: *encryption*] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]. *The standards shall be selected from the list of approved algorithms and parameters, in accordance with national guidance, and subject to each Certification Body. Notwithstanding, recommendations for algorithms and parameters for secure electronic signatures are given in [6].*

Application note: The TSF is used for the export of the Subscriber-SCD into the Subscriber-SSCD via a trusted channel (see FTP_ITC.1) to ensure its confidentiality and integrity. This TSF is also used to protect the integrity of the Subscriber-SVD during transfer from the TOE to the CGA and the Subscriber-SSCD. The integrity of the Subscriber-SCD and the Subscriber-SVD may be checked by verifying cryptographic relation between them. Note that the TOE must not create any signature with the Subscriber-SCD. The ST writer shall specify the algorithms used.

8.1.5 User Data Protection (FDP)

FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment: *RBAC-SFP*] on [assignment:

- *Subjects: users of the TOE.*
- *Objects: Subscriber-SCD, Subscriber-SVD, audit data, TSF data related to users and roles*
- *Operations: generate Subscriber-SCD and Subscriber-SVD pair, export (transmit) Subscriber-SCD and Subscriber-SVD, export (transmit) audit data, delete audit data, query one’s own RAD, users’ identity, roles and binding between users and roles, modify one’s own RAD, users’ identity, roles and binding between users and roles, and delete users’ identity, roles and binding between users and roles*].

FDP_ACF.1 Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [assignment: *RBAC-SFP*] to objects based on the following: [assignment:

- *Subjects: users of the TOE*
- *Objects; Subscriber-SCD, Subscriber-SVD, audit data, TSF data related to users and roles*
- *SFP-relevant security attributes: Identity and Role of the subject].*

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

(1) Users with Role Crypto-officer are allowed to:

Generate the objects Subscriber-SCD and Subscriber-SVD under, at least, dual person control.

export (transmit) the object Subscriber-SCD,

export (transmit) the object Subscriber-SVD,

export (transmit) audit data,

query one’s own RAD, users’ identity, roles and binding between users and roles,

modify one’s own RAD, users’ identity, roles and binding between users and roles, and

delete users’ identity, roles and binding between users and roles.

(2) Users with Role Auditor are allowed to:

Export (transmit) audit data,

delete audit data,

query one’s own RAD, and

modify one’s own RAD,].

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

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

(3) Users with Role Crypto-officer are not allowed to:

Delete audit data,

create a digital signature using the Subscriber-SCD,

query the RAD that belongs to a different user, and

modify the RAD that belongs to a different user.

(4) Users with Role Auditor, and, in general, any user holding a Role different than Crypto-officer, are not allowed to:

Generate the objects Subscriber-SCD and Subscriber-SVD,

create a digital signature using the Subscriber-SCD.

export (transmit) the object Subscriber-SCD,

export (transmit) the object Subscriber-SVD,

query users’ identity, roles and binding between users and roles,

modify users’ identity, roles and binding between users and roles,

delete users’ identity, roles and binding between users and roles,

create a digital signature using the Subscriber-SCD,

query the RAD that belongs to a different user, and

modify the RAD that belongs to a different user.].

Application note: The dual person control requires two users to be authenticated with different identities and with the same role Crypto-officer at the same time.

FDP_ETC.1 Export of user data without security attributes

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ETC.1.1 The TSF shall enforce the [assignment: *RBAC-SFP*] when exporting user data, controlled under the SFP(s), outside of the TOE.

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

FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *deallocation of the resource from*] the following objects: [assignment: *Subscriber-SCD*].

FDP_SDI.2 Stored data integrity monitoring and action

Dependencies: No dependencies.

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

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: *enter the secure state*].

Application note: The integrity of the Subscriber-SCD and the Subscriber-SVD may be checked by verifying cryptographic relation between them. Note that the TOE must not create any signature with the Subscriber-SCD.

FDP_UCT.1 Basic data exchange confidentiality

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_UCT.1.1 The TSF shall enforce the [assignment: *RBAC-SFP*] to [selection: *transmit*] user data in a manner protected from unauthorised disclosure.

Application note: This requirement shall be applied to any Subscriber-SCD when it is exported.

8.1.6 Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*]] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: *met, surpassed*], the TSF shall [assignment: *block the user's identity for authentication and close the session, if initiated*].

FIA_ATD.1 User attribute definition

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *Identity, assigned Role and RAD*].

FIA_SOS.1 Verification of secrets

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [assignment: *a defined quality metric*].

FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [assignment: *TOE start-up, TOE self-test, detection of the secure state, detection of violation of physical integrity, and identification*] on behalf of the user to be performed before the user is authenticated.

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

FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [assignment: *TOE start-up, TOE self-test, detection of the secure state, and detection of violation of physical integrity*] 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_USB.1 User-subject binding

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: *Identity and role*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *none*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *none*].

8.1.7 Security Management (FMT)

FMT_MOF.1 Management of security functions behaviour

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of*] the functions [assignment: *audit*] to [assignment: *Auditor*].

FMT_MSA.1 Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *RBAC-SFP*] to restrict the ability to [selection: *query, modify and delete*] the security attributes [assignment: users' identity, *roles and binding between users and roles*] to [assignment: *Crypto-officer*].

FMT_MSA.2 Secure security attributes

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [assignment: *users' identity, roles and binding between users and roles*].

FMT_MSA.3 Static attribute initialisation

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: *RBAC-SFP*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

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

FMT_MTD.1/Audit_trail Management of TSF data

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Audit_trail The TSF shall restrict the ability to [selection: *export*] the [assignment: *audit data*] to [assignment: *Auditor and Crypto-officer*].

FMT_MTD.1/Audit_trail_delete Management of TSF data

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Audit_trail The TSF shall restrict the ability to [selection: *delete*] the [assignment: *audit data*] to [assignment: *Auditor*].

FMT_SMF.1 Specification of Management Functions

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment:

- *Definition of the audit function behaviour*
- *User management*
- *Management of audit data*].

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *authorised identified roles, Crypto-officer and Auditor*].

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

Application note: A specific TOE may have defined additional roles. This is allowed as long as the definition of those roles is compliant with the requirements stated in this PP. Especially none of these additional roles shall have the ability to generate Subscriber-SCD/SVD or export Subscriber-SCD/SVD.

8.1.8 Privacy (FPR)

FPR_UNO.1 Unobservability

Dependencies: No dependencies.

FPR_UNO.1.1 The TSF shall ensure that [assignment: *Anybody*] are unable to observe the operation [assignment: *key generation, key destruction, encryption, signature generation computation*] on [assignment: *Subscriber-SCD*] by [assignment: *Crypto-officer*].

Application note: The TSF requires the TOE to prevent side-channel attacks against the Subscriber-SCD where the attack is based on external observable physical phenomena of the TOE. Please note that the encryption and signature generation computation operations listed in the SFR are not intended to use the Subscriber-SCD as the encryption/signing key, but rather the Subscriber-SCD is the data to be encrypted/signed. The TOE must not, under any circumstance, generate a digital signature using the Subscriber-SCD as the signing key. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the timing of transitions of internal states, the power consumption and the electromagnetic radiation. Such phenomena may be caused by normal internal operation of the TOE or may be forced by an attacker who varies the physical environment under which the TOE operates (e. g. power supply, temperature, radio emission or emission of light). Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation is assumed against state-of-the-art attacks applicable to the technologies employed by the TOE. Examples of such attacks are, but are not limited to, evaluation of the TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. The maximum capacity of the side channels should be defined by the ST allowing the CSP to prevent any remaining side channels by appropriate security measures in the TOE environment. The TSF requires the TOE to prevent side-channel attacks against the Subscriber-SCD through the intended output data of the TOE.

8.1.9 Protection of the TSF (FPT)

FPT_FLS.1 Failure with preservation of secure state

Dependencies: No dependencies.

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

- *Upon detection of a data integrity error detected in the user data stored in containers controlled by the TSF, as specified in FDP_SDI.2*
- *An error occurs during self tests specified in FPT_TST.1.*].

FPT_PHP.2 Notification of physical attack

Dependencies: FMT_MOF.1 Management of security functions behaviour

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For [assignment: *list of TSF devices/elements for which active detection is required*], the TSF shall monitor the devices and elements and notify [assignment: *users holding the role Crypto-Officer or Auditor*] when physical tampering *performed by opening the device or removal of a cover of* ~~with~~ the TSF's devices or TSF's elements has occurred.

Application note: The TOE environment should ensure that notification about physical tampering attempts given by the TOE is noticed by the CSP security personnel. The TOE non-IT environment should ensure that notification about physical tampering attempts given by the TOE is noticed by the CSP security personnel.

FPT_PHP.3 Resistance to physical attack

Dependencies: No dependencies.

FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering by opening the device or removal of a cover*] to the [assignment: *components which generate Subscriber-SCD/SVD pairs, store Subscriber SCD and store other secrets or private keys*] by responding automatically such that the SFRs are always enforced *and by secure deletion of Subscriber-SCD/Subscriber-SVD, keys used to establish the trusted channels and other confidential secret and private keys.*

FPT_RCV.1 Manual recovery

Dependencies: AGD_OPE.1 Operational user guidance

FPT_RCV.1.1 After [assignment: *list of failures/service discontinuities*] the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

FPT_STM.1 Reliable time stamps

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TST.1 TSF testing

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of self tests [selection: *during initial start-up, at the request of the authorised user, at the conditions* [assignment: *installation and maintenance*]], *initialization (extended software integrity test), power-up tests (software/firmware integrity test; Internal TSF data integrity test; cryptographic algorithm test; random number generator tests; critical functions test) and conditional tests (pair-wise consistency test (for public and private keys); manual key entry test (if manual key entry is implemented); continuous random number generator test)* to demonstrate the correct operation of [selection: [assignment: *parts of TSF*], *the TSF*].

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

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

Application note: The TSF performs self-tests according to FPT_TST.1 to ensure that the TOE is functioning properly. The extended software/firmware integrity test might verify error detecting codes, cryptographic checksums or digital signatures generated by the software/firmware developer or by other authorities. A digital signature might prove that the firmware or software is part of the evaluated product. The power-up software/firmware integrity test and internal TSF data integrity test may detect modification of these data if the device was switched off. The tests may be implemented by internally generated error detecting codes, cryptographic checksums or digital signatures. The cryptographic algorithm test may detect errors in hardware, firmware or software implementing critical cryptographic mechanisms (see FCS_CKM.1, FCS_COP.1). The test might be a known-answer-test (e.g. for encryption) or a pair-wise consistency test (e.g. verifying a SCD/SVD pair before the pair is exported). Supplementary tests shall detect error of the random number generator used for the generation of Subscriber-SCD (see FCS_CKM.1), cryptographic keys or parameters. If any critical function is not covered by these tests the TSF should implement additional self-tests. The pair-wise consistency test for public and private keys may detect errors in the key generation process. Other consistency tests may check the correctness of the signing process and other cryptographic processes to prevent e.g. differential fault attacks. Manual key entry test may detect errors to prevent use of incorrect keys if manual key entry is implemented. Continuous random number generator test may detect failure in operation of the generator to prevent use of wrong random number. The TOE shall verify the integrity of the TSF executable code at installation, maintenance and initialisation to prevent malicious software running on the TOE.

8.1.10 Trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

Dependencies: No dependencies.

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *the export of the Subscriber-SCD and the export of the Subscriber-SVD*].

Application note: The TOE shall provide a trusted channel between itself and either the Subscriber-SSCD or another trusted IT product that securely transfers the Subscriber-SCD to the Subscriber-SSCD. This trusted channel needs to protect the integrity and the confidentiality of the Subscriber-SCD. The trusted channel for the transfer of the Subscriber-SCD from the TOE to the Subscriber-SSCD shall ensure the confidentiality by means of cryptographic mechanisms as required by FCS_COP.1. Note that the encryption required by FCS_COP.1 may support but normally does not ensure by its own the integrity protection of the Subscriber-SCD. This trusted channel also needs to protect the integrity of the Subscriber-SVD during transfer from the TOE to the CGA and the Subscriber-SSCD.

FTP_TRP.1 Trusted path

Dependencies: No dependencies.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: [assignment: *modification and disclosure*].

FTP_TRP.1.2 The TSF shall permit [selection: *local users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication* [assignment:

- *Allowed controlled operations, as specified in FDP_ACF.1,*
- *operations available before the user is authenticated, as specified in FIA_UAU.1, and*
- *test operations, when requested by the local user, as specified in FPT_TST.1*].

Application note: Local users are those that interact with the TOE using the local interface (see Figure 1 — TOE Overview).

8.2 Security assurance requirements

The development and the evaluation of the TOE shall be done in accordance with security assurance requirements corresponding to the Evaluation Assurance Level 4 augmented (EAL4+) AVA_VAN.5.

Assurance Class	Assurance Component
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition

Assurance Class	Assurance Component
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Table 2 — Security Assurance Requirements: EAL4+ AVA_VAN.5

8.3 Security requirements rationale

8.3.1 Security functional requirements rationale

The following table shows the correspondence between the security objectives applicable to the TOE and the defined security functional requirements.

	O.Attack_Response	**O.Audit**	**O.Check_Operation**	**O.RBAC**	**O.Secure_State**	**O.Subscriber-SCD/SVD_Generation**	**O.Subscriber-SCD_Management**	**O.Subscriber-SVD_Management**	**O.User_Authentication**
FAU_GEN.1 Audit data generation		X							
FAU_GEN.2 User identity association		X							
FAU_STG.2 Guarantees of audit data availability		X							
FCS_CKM.1 Cryptographic key						X	X		

	O.Attack_Response	O.Audit	O.Check_Operation	O.RBAC	O.Secure_State	O.Subscriber-SCD/SVD_Generation	O.Subscriber-SCD_Management	O.Subscriber-SVD_Management	O.User_Authentication
generation									
FCS_CKM.4 Cryptographic key destruction							X		
FCS_COP.1 Cryptographic operation							X	X	
FDP_ACC.1 Subset access control				X					
FDP_ACF.1 Security attribute based access control				X					
FDP_ETC.1 Export of user data without security attributes				X					
FDP_RIP.1 Subset residual information protection							X		
FDP_SDI.2 Stored data integrity monitoring and action				X			X	X	
FDP_UCT.1 Basic data exchange confidentiality							X		
FIA_AFL.1 Authentication failure handling									X
FIA_ATD.1 User attribute definition				X					X
FIA_SOS.1 Verification of secrets									X
FIA_UAU.1 Timing of authentication			X		X				X
FIA_UID.1 Timing of identification			X		X				X
FIA_USB.1 User-subject binding				X					X
FMT_MOF.1 Management of security functions behaviour		X							

	O.Attack_Response	O.Audit	O.Check_Operation	O.RBAC	O.Secure_State	O.Subscriber-SCD/SVD_Generation	O.Subscriber-SCD_Management	O.Subscriber-SVD_Management	O.User_Authentication
FMT_MSA.1 Management of security attributes				X					X
FMT_MSA.2 Secure security attributes				X					
FMT_MSA.3 Static attribute initialisation				X					
FMT_MTD.1/Audit_trail Management of TSF data		X		X					
FMT_MTD.1/Audit_trail_delete Management of TSF data		X		X					
FMT_SMF.1 Specification of Management Functions		X		X					X
FMT_SMR.1 Security roles				X					X
FPR_UNO.1 Unobservability						X	X		
FPT_FLS.1 Failure with preservation of secure state					X		X	X	
FPT_PHP.2 Notification of physical attack	X						X	X	
FPT_PHP.3 Resistance to physical attack	X						X	X	
FPT_RCV.1 Manual recovery					X				
FPT_STM.1 Reliable time stamps		X							
FPT_TST.1 TSF testing	X		X		X				
FTP_ITC.1 Inter-TSF trusted channel							X	X	

	O.Attack_Response	O.Audit	O.Check_Operation	O.RBAC	O.Secure_State	O.Subscriber-SCD/SVD_Generation	O.Subscriber-SCD_Management	O.Subscriber-SVD_Management	O.User_Authentication
FTP_TRP.1 Trusted path							X		X

Table 3 — Mapping between Security Objectives and Security Functional Requirements

Security functional requirements (SFR) coverage is met as each security objective is addressed by at least one SFR, and every SFR is mapped to at least one security objective.

Next, the rationale for each matching is provided:

O.Attack_Response (Response to Physical Attacks) establishes that the TOE shall detect attempts of physical tampering and, in such cases, securely delete any R.SUBSCRIBER-SCD if this data has not already been deleted. To this end, **FPT_PHP.2 Notification of physical attack** permits the unambiguous detection and notification to the Crypto-officer of physical tampering. The detection is followed by the secure deletion of the Subscriber-SCD (**FPT_PHP.3 Resistance to physical attack**). The combination of both SFRs ensures that a physical attack is always detected and the Subscriber-SCDs are always deleted, guaranteeing its confidentiality. In addition, **FPT_TST.1 TSF testing** supports these two mechanisms by permitting the verification of the correct operation of the TSF, including those involved in the attack detection and Subscriber-SCD deletion.

O.Audit (Generation and Export of Audit Data) indicates that the TOE shall audit certain events, associate each auditable event with the identity of the user that caused the event. Also, the integrity of the audit trail shall be ensured, the TOE shall export the audit data upon request of the Auditor and the Crypto-officer, and the TOE shall provide the management function for the audit to the Auditor only. In this sense, SFRs **FAU_GEN.1 Audit data generation** and **FAU_GEN.2 User identity association** ensures that the TOE generates the required events and that the identity of the user that caused the event is associated with each auditable event. With this regard, **FPT_STM.1 Reliable time stamps** ensures that a reliable date and time are attached to each event generated, supporting subsequent audits. Also, **FAU_STG.2 Guarantees of audit data availability** indicates that the TOE shall protect the stored audit records from unauthorised deletion, guaranteeing the integrity of the audit trail. Respecting providing the management function for the audit to the Auditor only, this objective is met by requirements **FMT_MOF.1 Management of security functions behaviour** and **FMT_SMF.1 Specification of Management Functions**, with respect to the definition of the audit function's behaviour. On the other hand, **FMT_MTD.1/Audit_trail Management of TSF data** and **FMT_MTD.1/Audit_trail_delete Management of TSF data** permit both the Crypto-officer and the Auditor to export the audit data, while the deletion of the audit trails is restricted to the Auditor only.

O.Check_Operation (Check for Correct Operation) defines that the TOE shall perform regular checks to verify that its components operate correctly. To meet this objective, the TOE is provided with **FPT_TST.1 TSF testing**, by which the required checks are carried out during initial start-up, at the request of the authorised user, and at the installation and maintenance. **FIA_UAU.1 Timing of authentication** and **FIA_UID.1 Timing**

of identification support the execution of the TOE self tests before authentication and identification, respectively.

O.RBAC (Rol-based Access Control to TOE Services) establishes that the TOE shall restrict the access to its assets depending on the user role, allowing user access only to those services and data explicitly authorised to the assigned role. **FDP_ACC.1 Subset access control** defines the security policy for the access control, based on the subjects, the protected objects, and the operations that the subjects can perform on the objects. This policy is enforced based on the identity and role of the TOE user, as indicated by **FDP_ACF.1 Security attribute based access control**. Allowed roles are defined in **FMT_SMR.1 Security roles**. The RBAC security policy is supported by the secure management of users carried out by the Crypto-officer (**FMT_MSA.1 Management of security attributes, FMT_MSA.2 Secure security attributes, FMT_MSA.3 Static attribute initialisation** and **FMT_SMF.1 Specification of Management Functions**). **FIA_ATD.1 User attribute definition** ensures that the identity and role are associated to each individual user, permitting the retrieval of these security attributes and binding them with subjects acting on behalf the user after a successful authentication, as indicated by **FIA_USB.1 User-subject binding**. The RBAC security policy is enforced during any operation carried out by the user, including the export of user data (**FDP_ETC.1 Export of user data without security attributes**) and the access and management of audit data (**FMT_MTD.1/Audit_trail Management of TSF data** and **FMT_MTD.1/Audit_trail_delete Management of TSF data**). Finally, **FDP_SDI.2 Stored data integrity monitoring and action** ensures that if any security attribute needed to enforce the access control policy is modified, either inadvertently or on purpose without proper authorisation, then it is detected and the TSF enters the secure state.

O.Secure_State (Secure State in Case an Error is Detected) indicates that the TOE shall enter a secure state whenever it detects a failure or an integrity error of software, firmware, internal TSF data or user data, preventing the loss of confidentiality of any R.SUBSCRIBER-SCD. This objective is met by **FPT_FLS.1 Failure with preservation of secure state**, by which the TOE preserves a secure state when an error occurs during self tests specified in **FPT_TST.1 TSF testing**. Also, and by means of **FPT_RCV.1 Manual recovery**, if a failure or service discontinuity occurs (as specified by the ST writer), the TSF enters a maintenance mode where the ability to return to a secure state is provided. Finally, the user is able to detect if the TOE has entered a secure state as well as carry out self tests that may detect an incorrect or instable state before providing the credentials or before the authentication is established, as indicated by **FIA_UID.1 Timing of identification** and **FIA_UAU.1 Timing of authentication**, respectively.

O.Subscriber-SCD/SVD_Generation (Subscriber-SCD/SVD Pair Generation) defines that the TOE shall implement cryptographic algorithms and parameters compliant with the requirements established by the national authority for the R.SUBSCRIBER-SCD/ R.SUBSCRIBER-SVD pair generation. By **FCS_CKM.1 Cryptographic key generation**, the ST writer has to select the algorithms (including the algorithm used by the random number generator) from the list of approved algorithms and parameters, in accordance with national guidance, and subject to each Certification Body, and where recommendations for algorithms and parameters for secure electronic signatures are given in [6]. Secondly, **FPR_UNO.1 Unobservability** ensures that nobody is able to observe the Subscriber-SCD generation operation initiated by the Crypto-officer, enhancing the protection against disclosure by means of side-channel attacks.

O.Subscriber-SCD_Management (Secure Management of Subscriber-SCD) establishes that the TOE shall ensure the confidentiality and integrity of the R.SUBSCRIBER-SCD both when it is under the control of the TOE and during transfer from the TOE to the Subscriber-SSCD, and that the R.SUBSCRIBER-SCD shall be securely deleted from the TOE whenever it is exported. In general, the confidentiality of the R.SUBSCRIBER-SCD is ensured by using strong algorithms that prevent from partial or total derivation (**FCS_CKM.1 Cryptographic key generation**). Within the boundaries of the TOE, the R.SUBSCRIBER-SCD is protected by a secure deletion of the keys once it has been successfully imported to the Subscriber-SSCD (**FCS_CKM.4 Cryptographic key destruction**), or when an error has occurred. With this regard, **FPT_FLS.1 Failure with preservation of secure state** preserves the secure state where an error occurs, while **FPT_PHP.2 Notification of physical attack** and **FPT_PHP.3 Resistance to physical attack** support the detection and immediate deletion of the R.SUBSCRIBER-SCD in the case that a physical attack occurs. In both cases (deletion after import or deletion after error/attack detection) the unavailability of the Subscriber-SCD after the deallocation of the resource is ensured by **FDP_RIP.1 Subset residual information protection**. More specifically, any error regarding the integrity of the R.SUBSCRIBER-SCD when managed within the TOE boundaries is ensured by **FDP_SDI.2 Stored data integrity monitoring and action**. Respecting the protection of the R.SUBSCRIBER-SCD when sent out of the TOE boundaries, different SFRs apply. The channel used to transmit the R.SUBSCRIBER-SCD to the third parties and the Subscriber-SSCD is protected by **FTP_ITC.1 Inter-TSF trusted channel**, which ensures confidentiality and integrity. Also, local users (i.e. Crypto-officers) can invoke the export operation of R.SUBSCRIBER-SCD by using the local interface provided by the TOE. The TOE, by means of **FTP_TRP.1 Trusted path**, provides a logically distinct communication path between itself and local users that protects the communicated data from modification and disclosure. In addition to this, **FDP_UCT.1 Basic data exchange confidentiality** prevents the unauthorised disclosure of the R.SUBSCRIBER-SCD by enforcing the RBAC-SFP when it is exported through the trusted channel. FDP_UCT.1 also enforces the RBAC-SFP to transmit any other user data that may be exchanged with the local users through the aforementioned communication path. When encryption of data is needed before transmission through the trusted channel in order to ensure confidentiality and integrity of R.SUBSCRIBER-SCD, the encryption has to be undertaken according to **FCS_COP.1 Cryptographic operation**. Finally, **FPR_UNO.1 Unobservability** ensures that nobody is able to observe any key destruction, encryption or digital signature operation initiated by the Crypto-officer and performed on the Subscriber-SCD, enhancing the protection against disclosure by means of side-channel attacks.

O.Subscriber-SVD_Management (Secure Management of Subscriber-SVD) specifies that the TOE shall ensure the integrity of the R.SUBSCRIBER-SVD both when it is under the control of the TOE and during transfer from the TOE to the CGA or the Subscriber-SSCD. The justification of compliance is similar to the case above, but focused on the integrity property. In this case, any error regarding the integrity of the R.SUBSCRIBER-SVD when managed within the TOE boundaries is ensured by **FDP_SDI.2 Stored data integrity monitoring and action**. **FPT_FLS.1 Failure with preservation of secure state** preserves the secure state where an error occurs, while **FPT_PHP.2 Notification of physical attack** and **FPT_PHP.3 Resistance to physical attack** support the detection and immediate deletion of the R.SUBSCRIBER-SVD in the case that a physical attack occurs (e.g. an attack that intends to modify the R.SUBSCRIBER-SVD). Finally, **FTP_ITC.1 Inter-TSF trusted channel** protects the data exchanged between the TOE and the Subscriber-SSCD and the CGA in integrity, while **FCS_COP.1 Cryptographic operation** is used to cryptographically protect such integrity of the R.SUBSCRIBER-SVD.

O.User_Authentication (Authentication of TOE Users) indicates that the TOE shall be able to identify and authenticate the users (based on user identity) acting with a defined role, before allowing any access to TOE protected assets. **FIA_UID.1 Timing of identification** and **FIA_UAU.1 Timing of authentication** enforce the identification and authentication of the TOE users before allowing them execute TSF-mediated actions that are not explicitly allowed in the corresponding SFRs. For a correct authentication, the VAD provided by the user should be verified against the RAD. **FIA_ATD.1 User attribute definition** permits maintaining a list of security attributes (including the user’s identity and RAD) for each individual user, what is the pillar for an identity-based authentication mechanism. In addition, **FIA_USB.1 User-subject binding** establishes the association of the user’s identity with the subject acting on behalf of that user. It should be noted that the maximum number of authentication attempts is restricted by **FIA_AFL.1 Authentication failure handling**. The secrets used by the users to identify themselves are verified against quality metrics by **FIA_SOS.1 Verification of secrets**. The ability to manage the user accounts, including the users' identities and roles, is established by **FMT_MSA.1 Management of security attributes** and **FMT_SMF.1 Specification of Management Functions**, whereas **FMT_SMR.1 Security roles** is aimed at maintaining the roles and establishing the association between users and roles. Finally, local users that connect to the TOE are provided with a trusted path to permit a secure identification and authentication processes. This is endorsed by **FTP_TRP.1 Trusted path**.

8.3.2 Security assurance requirements rationale

The Security Assurance Requirements (SAR) for this Protection Profile have been selected according to the Evaluation Assurance Level 4 augmented (EAL4+) AVA_VAN.5.

EAL4+ AVA_VAN.5 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+ AVA_VAN.5 is appropriate for commercial products that can be applied to moderate to high security functions, and resist to high attack potential. The TOE described in this Protection Profile is such a product.

Bibliography

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 3. CCMB-2009-07-001, July 2009

[3] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 3. CCMB-2009-07-002, July 2009

[4] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 3. CCMB-2009-07-003, July 2009

[5] Common Criteria portal. Available at http://www.commoncriteriaportal.org/

[6] ETSI TS 102 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures

[7] ISO/IEC 13888-3, Information technology -- Security techniques -- Non repudiation -- Part 3: Mechanisms Using Asymmetric Techniques. International Organization for Standardization, 2009

[8] ETSI TS 101 456 Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates, V1.4.3, May 2007

[9] EN 14169-3 Protection Profile for Secure Signature Creation Device Part 3: Device with key import.