CEN

WORKSHOP

AGREEMENT

CWA 14167-3

May 2004

English version

Cryptographic module for CSP key generation services protection profile CMCKG-PP

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN members are the national standards bodies of Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Switzerland and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

Management Centre: rue de Stassart, 36   B-1050 Brussels

—— this page has intentionally been left blank ——

Foreword

This 'Cryptographic Module for CSP Key Generation Services - Protection Profile' (CMCKG-PP) is issued by the European Committee for Standardization, Information Society Standardization System (CEN/ISSS) Electronic Signatures (E-SIGN) workshop. The document represents the CEN/ISSS workshop agreement (CWA) on trustworthy systems area D2.

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] as generally recognised standard for electronic-signature products in the Official Journal of the European Communities.

This document supersedes CWA 14167-3:2003.

The document has been prepared as a Protection Profile (PP) following the rules and formats of the Common Criteria version 2.1 [2] [3] [4]. This PP has not been evaluated.

The set of algorithms for secure signature-creation devices and parameters for algorithms for secure signature-creation devices is given in a separate document [5].

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

CONTACT ADDRESS

CEN/ISSS WS/E-Sign Project Team Maintenance
Editor: Wolfgang Killmann
Email: Wolfgang.Killmann@t-systems.com

After CWA approval the contact address will be:

CEN/ISSS Secretariat
Rue de Stassart 36
1050 Brussels, Belgium

Tel   +32 2 550 0813
Fax   +32 2 550 0966

Email   isss@cenorm.be

—— this page has intentionally been left blank ——

Revision History

PRE-RELEASE HISTORY FOR EDITORIAL TRACKING ONLY, REPLACE FOR FINAL PP

v0.01   17.12.01   initial draft

v0.02   15.01.02   second draft, includes drafts of chapter 3 to 5

v0.03   25.01.02   third draft, includes discussion of the Barcelona meeting

v0.04 - v0.06   working drafts

v0.07   24.07.02   draft for public comments

v0.08   13.09.02   draft with changes according to public comments

v0.09   03.06.03   editorial changes due to maintenance, adoption to draft PP CMCSO and PP CMCSOB for compatibility

v010   21.11.03   changes due to maintenance, adoption to draft PP CMCSO and PP CMCSOB for compatibility

v011   28.01.04   typos corrected, some adoption to draft PP CMCSO and PP CMCSOB for compatibility

v012   12.02.04   editorial refinements according to received comments

—— this page has intentionally been left blank ——

Table of Contents

List of Tables

—— this page has intentionally been left blank ——

Conventions and Terminology

Conventions

The document follows the rules and conventions laid out in Common Criteria 2.1, part 1 [2], Annex B "Specification of Protection Profiles". Admissible cryptographic algorithms and parameters for algorithms are given in a separate document [5]. Therefore, the Protection Profile (PP) refers to [5].

Terminology

Administrator means a CSP user role that performs TOE initialisation or other TOE administrative functions. These tasks are mapped to the Crypto-officer role of the TOE.

Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:
- (a)   it is uniquely linked to the signatory;
- (b)   it is capable of identifying the signatory;
- (c)   it is created using means that the signatory can maintain under his sole control, and
- (d)   it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Authentication data is information used to verify the claimed identity of a user.

Auditor means a user exporting the TOE audit data and reviewing the audit data with tools in the TOE environment.

CEN workshop agreement (CWA) is a consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN).

Certificate means an electronic attestation which links the SVD to a person and confirms the identity of that person. (defined in the Directive [1], article 2.9)

Certification generation application (CGA) means a collection of application elements which requests the SVD from the device generating the SCD/SVD pair for generation of the qualified certificate. The CGA stipulates the generation of a correspondent SCD / SVD pair, if the requested SVD has not been generated by the SCD/SVD generation device yet. The CGA verifies the authenticity of the SVD by means of
- (a)   the SSCD proof of correspondence between SCD and SVD and
- (b)   checking the sender and integrity of the received SVD.

Certification-service-provider (CSP) means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures (defined in the Directive [1], article 2.11).

Digital signature means data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO 7498-2]

Directive 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] is also referred to as the 'Directive' in the remainder of the PP.

Hardware security module (HSM) means the cryptographic module used to generate the Subscriber-SCD/Subscriber-SVD pair and which represents the TOE.

List of approved algorithms and parameters means cryptographic algorithms and parameters published in [5] for electronic signatures, secure signature creation devices and trustworthy systems

Qualified certificate means a certificate which meets the requirements laid down in Annex I of the Directive [1] and is provided by a CSP who fulfils the requirements laid down in Annex II of the Directive [1]. (defined in the Directive [1], article 2.10)

Reference authentication data (RAD) means data persistently stored by the TOE for verification of the authentication attempt as authorised user.

Secure signature-creation device (SSCD) means configured software or hardware which is used to implement the SCD and which meets the requirements laid down in Annex III of the Directive [1]. (SSCD is defined in the Directive [1], article 2.5 and 2.6).

Secure signature-creation device Type 2 (SSCD Type 2) means a SSCD that is used by the signatory for signature-creation, but which does not create Subscriber-SCD itself. The Subscriber-SCD is exported by the TOE to the SSCD Type 2. (Note: The notion of an 'SSCD Type 2' has been taken from the SSCD-PP [7].)

Side-channel means illicit information flow in result of the physical behaviour of the technical implementation of the TOE. Side-channels are but limited to interfaces not intended for data output like power consumption, timing of any signals and radiation. Side-channels might be enforced by influencing the TOE behaviour from outside.

Signature-creation data (SCD) means 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)

Signature-verification data (SVD) means 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 2.7)

SSCD provision service means a service that prepares and provides a SSCD to subscribers.

Subscriber Signature-Creation Data (Subscriber-SCD) means SCD which is used by the Subscriber (the signatory) for the creation of qualified electronic signatures by means of a SSCD.

Subscriber Signature-Verification Data (Subscriber-SVD) means SVD which corresponds to the Subscriber-SCD and which is used to verify the qualified electronic signature.

System auditor of the CSP is a role in the IT environment of the TOE (certification service provider) authorised to view archives and audit logs of trustworthy systems.

User means any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data means data created by and for the user that does not affect the operation of the TSF.

Verification authentication data (VAD) means authentication data provided as input by knowledge or authentication data derived from user's biometric characteristics.

Document Organisation

Section 1 provides the introductory material for the Protection Profile.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware, the TOE software, or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional requirements and assurance requirements derived from the Common Criteria (CC), Part 2 [3] and Part 3 [4], that must be satisfied by the TOE.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements

A reference section is provided to identify background material.

An acronym list is provided to define frequently used acronyms.

1 Introduction

This section provides document management and overview information that is required to carry out protection profile registry. Therefore, section 1.1 "Identification" gives labelling and descriptive information necessary for registering the Protection Profile (PP). Section 1.2 "Protection Profile Overview" summarises the PP in narrative form. As such, the section gives an overview to the potential user to decide whether the PP is of interest. It is usable as stand-alone abstract in PP catalogues and registers.

1.1 Identification

Title:	Cryptographic Module for CSP Key Generation Services – Protection Profile
Authors:	Wolfgang Killmann, Herbert Leitold, Hans Nilsson
Vetting Status:	
CC Version:	2.1 Final
General Status:	WS/E-Sign draft for public comments
Version Number:	0.12
Registration:	
Keywords:	cryptographic module, CSP, key generation

The following final interpretation of the CCIMB related to APE criteria in CC part 3 [4] and the CEM [8] were taken into account: 008, 013, 019, 043, 051, 049, 058, 064, 065, 084, 085, 098, 138.

1.2 Protection Profile Overview

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 PP, 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) [1] issuing Qualified Certificates" (ETSI TS 101 456) [6], it is stated that

The CA shall ensure that any subscriber keys, that it generates, are generated securely and the privacy of the subscriber's private key is assured (see [1], annex II (f) and annex II (j)).

---

[1] Note: 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.

and

a) *CA-generated subscriber keys shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures.*
b) *CA-generated subscriber 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.*
c) *CA-generated subscriber keys shall be generated and stored securely before delivery to the subscriber.*
d) *The subscriber's private key shall be delivered to the subscriber in a manner such that the privacy of the key is not compromised and on delivery only the subscriber has access to its private key.*

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 (Subscriber-SCD). A cryptographic module for CSP key generation services is needed particularly for initialisation of SSCD Type 2 [7].

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 Protection Profile.

This PP is Part 2 extended and Part 3 conformant. The assurance level for this PP is EAL4, augmented with ADV_IMP.2 (implementation of the TSF), AVA_CCA.1 (vulnerability assessment, covert channel analysis) and AVA_VLA.4 (vulnerability assessment, highly resistant). The minimum strength level for the TOE security functions is 'SOF high' (Strength of Functions High).

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 Protection Profile 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.

2 TOE Description

The TOE is a Cryptographic Module (CM) used for the creation of Signature Creation Data (Subscriber-SCD) / Signature Verification Data (Subscriber-SVD) pairs and loading of these into Secure Signature Creation Devices (SSCD) such that the confidentiality of the Subscriber-SCD is maintained.

The TOE shall provide the following additional functions to protect these cryptographic functions:

- User authentication
- Access control for use of the Subscriber-SCD/SVD generation and export function
- 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 subscribers, created internally in the TOE and loaded into an SSCD
- Subscriber Signature Verification Data (Subscriber-SVD): public key of subscriber, created internally in the TOE and transferred into an SSCD, to an CGA, or to both, This data may also be distributed to additional entities.

2.1 TOE Roles

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

- Crypto-officer (authorized to install, configure and maintain the TOE, 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. 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.

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.

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

2.2   TOE Usage

In most cases the TOE will be a separate component with its own hardware and software, communicating via a well-defined physical and logical interface with the client application. Examples of physical interfaces that may be used to connect the TOE to the client application are the PCI bus, the SCSI bus, USB or Firewire.

Logically the TOE is responsible for protecting the Subscriber-SCD against disclosure, compromise and unauthorized modification and for ensuring that the TOE services are only used in an authorized way.
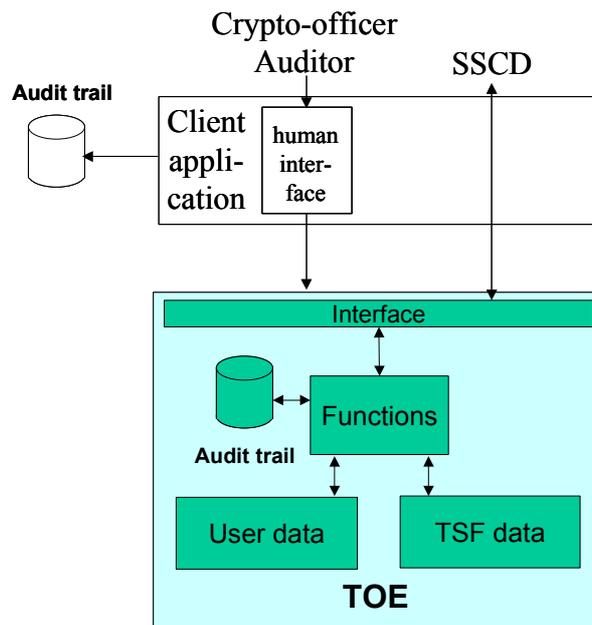
Figure 1: TOE general overview

The TOE is used to generate Subscriber-SCD/SVD pairs for cryptographic algorithms and key sizes approved for the use for qualified electronic signatures in accordance with the EU directive. The TOE shall provide a function to export the Subscriber-SCD / Subscriber-SVD pairs for the integration into the SSCD of subscribers. The confidentiality of the Subscriber-SCD as well as the integrity and authenticity of both the Subscriber-SCD and the Subscriber-SVD needs to be protected during the transfer from the TOE to a Subscriber-SSCD.

Application Note:

This Protection Profile will not define the mechanism that is used to establish such a trusted channel between the TOE and the SSCD. It also does not demand that there is an on-line connection between the TOE and the SSCD. The communication may also be off-line, but in any case the requirements for the protection of the Subscriber-SCD during transfer and the requirements to protect a single Subscriber-SCD against import into and use by more than one SSCD have to be satisfied. These requirements are derived from the following statement within ETSI TS 101 456 V1.1.1 (2000-12): *"The subscriber's private key shall be delivered to the subscriber in a manner such that the privacy of the key is not compromised and on delivery only the subscriber has access to its private key."*

3 TOE Security Environment

3.1 Assets to protect

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

TOE services

- **R.SERVICES**: integrity and availability of the TOE services as well as protection against misuse is required.

TOE internal data:

- **R. SUBS_DATA**: data the TOE generates for a subscriber. This is the Subscriber-SCD and the Subscriber-SVD. Subscriber-SCD has to be protected both in confidentiality and in integrity, Subscriber-SVD has to be protected in integrity.

- **R.USERMGMT_DATA**: non-confidential user / role related data (identifier, access control lists, role definitions, etc.). Those data has to be protected in integrity.

- **R. SYSTEM_DATA**: TSF data (especially VAD and RAD) and other system data not related to a user or role (system configuration data, audit data) which have to be protected in confidentiality, integrity and availability.

3.2 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 according to the audit procedure of the CSP.

A.Human_Interface   *Interface with Human Users*

The client application will provide an appropriate interface and communication path between human users and the TOE because the TOE does not have a human interface for authentication and management services. The TOE environment transmits identification, authentication and management data of TOE users correctly and in a confidential way to the TOE.

3.3 Threats to Security

T.Bad_SW Malicious Software during the Lifetime of the TOE

When the TOE provides the ability to load new software or software updates or to modify software when it is in operation, this function can be misused to load malicious software by unauthorised persons.

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

The most valuable asset the TOE has to protect are the Subscriber-SCDs it generates. The ability to derive all or parts of Subscriber-SCD in any way (including the legitimate use of the TOE services) presents a threat that needs to be countered by the TOE. This includes also any ability to derive all or part of the Subscriber-SCD using knowledge about the key generation process.

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

Direct disclosure of Subscriber-SCD or part of it presents a major threat to the TOE. This includes any way of disclosing all or part of the Subscriber-SCD generated by the TOE over any physical or logical TOE interface.

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

A Subscriber-SCD generated by the TOE may be transferred to more than one SSCD which may result 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.SVD_Forgery *Forgery of the signature-verification data*

An attacker forges the SVD exported by the TOE during the transmission to the CGA or to the SSCD for storing and later transmission from the SSCD to the CGA. This result in loss of SVD integrity in the certificate of the signatory.

T.Malfunction *Malfunction of TOE*

Internal malfunction of TOE functions may result in the generation of Subscriber-SCD of low quality or invalid Subscriber-SCD, misuse of TOE services, disclosure of Subscriber-SCD or denial of service for authorised users.

The correct operation of the TOE also depends on the correct operation of critical hardware components. A failure of such a critical hardware component could result in the disclosure or distortion of secret keys, or the ability to misuse services of the TOE. Technical failure may result in a insecure operational state violating the integrity and availability of the TOE services. Critical components might be:

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

T.Insecure_Init   *Insecure Initialisation of the TOE*

Unauthorised CSP personnel or authorised CSP personnel without using adequate organisational controls may initialise the TOE with insecure system data, management data or user data.

T.Insecure_Oper   *Insecure Operation of the TOE*

The TOE may be operated in an insecure way not detectable by the TOE itself. This includes the use and operation of the TOE within another environment than the intended one (e. g. the TOE may be connected to a hostile system).

T.Management   *Misuse of Management*

CSP personnel may misuse the TOE services to forge user data as Subscriber-SCD, Subscriber-SVD, user management data, system data or TSF data.

T.Misuse   *Misuse of Subscriber-SCD/SVD pair generation function*

An attacker misuses the TOE for generation of Subscriber-SCD/SVD pairs. This may result in Subscriber-SCD/SVD pairs that are used without proper authorization.

T.Phys_Manipul   *Physical Manipulation of the TOE*

An attacker may try to physically manipulate the TOE with the intent to derive all or part of the Subscriber-SCD and Subscriber-SVD or to misuse services of the TOE. The TOE may be physically attacked by even an authorised user of TOE services.

3.4   Organisational Security Policies

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

Only algorithms and algorithm parameter defined as acceptable for being used in Subscriber-SCD/SVD pair generation for secure electronic signatures. This includes the generation of random numbers and the quality of the Subscriber-SCD/SVD pairs generated. A list of approved algorithms and parameters is given in [5].

Where confidentiality protection is required such as for the transfer of Subscriber-SCD to the Subscriber-SSCD, only cryptographic strong algorithms and algorithm parameters shall be used.

4 Security Objectives

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

4.1 Security Objectives for the TOE

O.Audit_CM *Generation and Export of Audit Data*

The TOE shall audit the following events:

- TOE initialisation
- TOE start-up
- Generation of Subscriber-SCD/SVD pairs
- Unsuccessful authentication
- Modification of TOE 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, at the request of the authorised user, at the conditions installation and maintenance
- Exporting and deleting audit trail records

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.Subs-SCD_Secure *Secure Subscriber-SCD Generation and Management*

The confidentiality and integrity of the Subscriber-SCD shall be ensured as long as they are under the control of the TOE. The TOE shall ensure cryptographic secure Subscriber-SCD/SVD pair generation and transfer to the Subscriber-SSCD. This includes protection against disclosing completely or partly the Subscriber-SCD in clear through any physical or logical TOE interface. The TOE shall not use any Subscriber-SCD for signature creation. The TOE implements secure cryptographic algorithms and parameters for the Subscriber-SCD/SVD pair generation chosen from [5].

O.Check_Operation *Check for Correct Operation*

The TOE shall perform regular checks to verify that its components operate correctly. This includes integrity checks of TOE software, firmware, internal TSF data or user data during initial start-up, at the request of the authorised user, at the conditions installation and maintenance.

O.Control_Services   *Management and Control of TOE Services*

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

O.Detect_Attack   *Detection of Physical Attacks*

The TOE shall detect attempts of physical tampering and securely destroy any Subscriber-SCD in case this data has not already been destroyed.

O.Error_Secure   *Secure State in Case an Error is detected*

The TOE shall enter a secure state whenever it detects an 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 Subscriber-SCD.

O.SCD_Transfer   *Secure export of Subscriber-SCD to the SSCD*

The TOE shall ensure the confidentiality of the Subscriber-SCD transferred from the TOE to a SSCD via a trusted channel. The Subscriber-SCD shall be deleted from the TOE whenever it is exported from that TOE.

O.SVD_Transfer   *Secure export of SVD to CGA or SSCD*

The TOE shall ensure the integrity of the Subscriber-SVD exported to the CGA or to the SSCD via a trusted channel.

O.User_Authentication   *Authentication of Users interacting with the TOE*

The TOE shall be able to identify and authenticate the users acting with a defined role, before allowing any access to TOE protected assets. Identification and authentication shall be user-based.

4.2   Security Objectives for the Environment

The following security objectives relate to the TOE environment. This includes the client application as well as the procedures for the secure operation of the TOE

O.ENV_Audit   *Audit review*

The environment provides a review of the audit trail recorded by the TOE.

O.ENV_Human_Interface   *Reliable Human Interface*

If the client application provides a human interface and a communication path between human users and the TOE, the client application will ensure the confidentiality and integrity of the data transferred between the TOE and the human user.

O.ENV_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.

O.ENV_Protect_Access   *Prevention of Unauthorised Physical Access*

The TOE shall be protected by physical, logical and organisational protection measures, 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.

O.ENV_Secure_Init   *Secure Initialisation Procedures*

Procedures and controls in the TOE environment shall be defined and applied that allow to securely set-up and initialise the TOE for the generation Subscriber-SCD/-SVD pair . This includes the initial configuration of other TSF data like roles, users and user authentication information.

O.ENV_Secure_Oper   *Secure Operating Procedures*

Procedures and controls in the TOE environment shall be defined that allow operating the TOE within a CA system in compliance with the requirements of the EU directive and the Policy for certification authorities issuing qualified certificates.

O.ENV_SCD_Transfer   *Secure import of Subscriber-SCD to SSCD*

The SSCD shall support the cryptographic protection of the Subscriber-SCD during the transfer from the TOE and ensure the confidentiality of the Subscriber-SCD under its control.

O.ENV_SVD_Transfer   *Secure import of SVD to CGA or SSCD*

The CGA or the SSCD importing the SVD exported by the TOE shall ensure the integrity of the SVD.

5 IT Security Requirements

This chapter gives the security functional requirements (SFR) and the security assurance requirements (SAR) for the TOE and the environment.

Security functional requirements components given in section 5.1 "TOE security functional requirements" are drawn from Common Criteria part 2 [3]. Some security functional requirements represent extensions to [3], with a reasoning given in section 6.5. Operations for assignment, selection and refinement have been made. Operations not performed in this PP are identified in order to enable instantiation of the PP to a Security Target (ST).

The TOE security assurance requirements statement given in section 5.2 "TOE Security Assurance Requirement" is drawn from the security assurance components from Common Criteria part 3 [4].

Section 5.3 identifies the IT security requirements that are to be met by the IT environment of the TOE.

The non-IT environment is described in section 5.4.

5.1 TOE Security Functional Requirements

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1)

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 <u>not specified</u> level of audit; and
- c) <u>Initialisation of the TOE,
  Start-up after power-up,
  Shutdown of the TOE,
  Software download if supported by the TOE,
  Cryptographic key generation (FCS_CKM.1): Subscriber-SCD/CSP-SVD pair generation,
  Cryptographic key destruction (FCS_CKM.4): destruction of keys used to establish the trusted channel (FCS_CKM.4),
  Export of user data without security attributes (FDP_ETC.1): number of keys exported,
  Authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts and the actions,
  Timing of authentication (FIA_UAU.1): all unsuccessful use of the authentication mechanism,
  Management of security attributes (FMT_MSA.1) /(all instantiations): all modifications of the values of security attributes,</u>

Static attribute initialisation (FMT_MSA.3): modifications of the default setting of permissive or restrictive rules, all modifications of the initial values of security attributes;
Management of TSF data (FMT_MTD.1/ACCESS_CONTROL): All modifications to the values of TSF data,
Management of TSF data (FMT_MTD.1/AUDIT: Export of audit data, Clear of audit data,
Abstract machine testing (FPT_AMT.1): Execution of the tests of the underlying machine and the results of the tests,
Failure with preservation of secure state (FPT_FLS.1): Failure detection of the TSF and secure state,
Notification of physical attack (FPT_PHP.2): Detection of intrusion,
TSF testing (FPT_TST.1): Execution of the TSF self tests and during initial start-up, at the request of the authorised user, at the conditions installation and maintenance, unsuccessful self test operations,
Inter-TSF trusted channel (FTP_ITC.1): Initialisation of communication via the trusted channel

FAU_GEN.1.2   The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, identity of the user and sequence data

Refined by adding:
Date and time of the event may be given by the sequence data correlated to time of export the audit data to the TOE environment. The sequence data shall be a sequence number of the audit event data or time stamp.

Application note:
If time stamps are chosen as the sequence data the ST shall include security functional requirements for reliable time stamps (FPT_STM.1).

5.1.1.2   User identity association (FAU_GEN.2)

FAU_GEN.2.1   The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3   Guarantees of audit data availability (FAU_STG.2/TOE)

FAU_STG.2.1/TOE The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2/TOE The TSF shall be able to prevent modifications to the audit records.

FAU_STG.2.3/TOE   The TSF shall ensure that [assignment: metric for saving audit records] audit records will be maintained when the following conditions occur: audit storage exhaustion.

Application note:
The TSF may overwrite the audit trail data after reading (export) by the Auditor. The ST 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.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic key generation (FCS_CKM.1)

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*].

Refined by adding:
The standards for cryptographic key generation shall be assigned from the list of approved algorithms and parameters [5].

Application note:
The SFR FCS_CKM.1 describes the generation of the Subscriber-SCD. The ST writer should iterate FCS_CKM.1 if the TOE shall generate cryptographic keys used by TSF according to FCS_COP.1 and FDP_UCT.1 for the transfer of the Subscriber-SCD over the trusted channel according to FTP_ITC.1. Note that [5] does not list any key generation algorithm for encryption.

5.1.2.2 Cryptographic key destruction (FCS_CKM.4)

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:
The TSF will destroy Subscriber-SCD immediately after the TSF has exported the Subscriber-SCD. The TSF will destroy the Subscriber-SCD and all other plaintext secret or private keys, if the TSF required by FPT_PHP.2 detects physical tampering. The security of the key destruction is subject of the information flow control required by FDP_IFF.4 and the covered channel analysis AVA_CCA.1. The TOE will destroy also the key used by TSF according to FCS_COP.1

and FDP_UCT.1 for the transfer of the Subscriber-SCD over the trusted channel according to FTP_ITC.1.

5.1.2.3   Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/
SCD Export
The TSF shall perform <u>encryption</u> 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*].

Application note:
The TSF will be used for the export of the Subscriber-SCD into the Subscriber-SSCD via a trusted channel (see FTP_ITC.1/SCD_Export and FPT_ITC.1/SCD_Import) to ensure the confidentiality according to FDP_UCT.1.

5.1.2.4   Quality metrics for random numbers (FCS_RND.1)

FCS_RND.1.1
The TSF shall provide a mechanism for generating random numbers that meet [assignment: *a defined quality metric*].

FCS_RND.1.2
The TSF shall be able to enforce the use of TSF-generated random numbers for <u>FCS_CKM.1</u>.

Application Note:
The quality metric shall meet the requirements defined for Subscriber-SCD/SVD generation in the list of approved algorithms and parameters [5].

5.1.3   User data protection (FDP)

5.1.3.1   Subset access control (FDP_ACC.1/CRYPTO)

FDP_ACC.1.1/
CRYPTO
The TSF shall enforce the <u>Crypto-SFP</u> on <u>User; Subscriber-SCD, Subscriber-SVD; generate Subscriber-SCD/SVD pair (FCS_CKM.1), destruction of Subscriber-SCD and Subscriber-SVD (FCS_CKM.4)</u>.

5.1.3.2   Subset access control (FDP_ACC.1/AUDIT)

FDP_ACC.1.1/
AUDIT
The TSF shall enforce the <u>Audit-SFP</u> on <u>User; Audit data; export and delete</u>.

5.1.3.3 Security attribute based access control (FDP_ACF.1/CRYPTO)

FDP_ACF.1.1/
CRYPTO

The TSF shall enforce the <u>Crypto-SFP</u> to objects based on <u>Identity and Role</u>.

FDP_ACF.1.2/
CRYPTO

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
   (1) <u>User with security attribute Role Crypto-Officer is allowed to generate (FCS_CKM.1) the objects Subscriber-SCD and Subscriber-SVD</u>
   (2) <u>User with security attribute Role Crypto-Officer is allowed to export (FDP_UCT.1, FTP_ITC.1) the object Subscriber-SCD.</u>
   (3) <u>User with security attribute Role Crypto-Officer is allowed to export (FTP_ITC.1) the object Subscriber-SVD</u>

FDP_ACF.1.3/
CRYPTO

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: <u>none</u>.

FDP_ACF.1.4/
CRYPTO

The TSF shall explicitly deny access of subjects to objects based on the <u>following rules: User with security attribute Auditor is not allowed to</u>
   (a) <u>generate (FCS_CKM.1) the objects Subscriber-SCD and Subscriber-SVD,</u>
   (b) <u>export (FDP_UCT.1, FTP_ITC.1) the objects Subscriber-SCD and Subscriber-SVD.</u>

5.1.3.4 Security attribute based access control (FDP_ACF.1/AUDIT)

FDP_ACF.1.1/
AUDIT

The TSF shall enforce the <u>Audit-SFP</u> to objects based on <u>Identity and Role</u>.

FDP_ACF.1.2/
AUDIT

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
   <u>(1) Users with the role attribute Auditor are allowed</u>
      <u>(a) to export Audit data,</u>
      <u>(b) to delete Audit data</u>.
   <u>(2) Users with security attribute Role Crypto-officer are allowed to export Audit data</u>.

FDP_ACF.1.3/
AUDIT

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: <u>none</u>.

FDP_ACF.1.4/
AUDIT

The TSF shall explicitly deny access of subjects to objects based on the rule: <u>Users with security attribute Role Crypto-officer are not allowed to delete Audit data.</u>

5.1.3.5   Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1   The TSF shall enforce the <u>Side-channels of Crypto-functions SFP on Anybody; Information about Subscriber-SCD; generation of Subscriber-SCD/SVD pair (FCS_CKM.1), destruction of Subscriber-SCD (FCS_CKM.4) and Subscriber-SCD transfer (FPT_ITC.1)</u>.

5.1.3.6   Partial elimination of illicit information flows (FDP_IFF.4)

FDP_IFF.4.1   The TSF shall enforce the <u>Side-channels of Crypto-functions SFP</u> to limit the capacity of <u>side-channels of the Subscriber-SCD/SVD generation (FCS_CKM.1) through physical behaviour of the TOE interfaces and emanation compromising information about the Subscriber-SCD</u> to a [assignment: *maximum capacity*].

FDP_IFF.4.2   The TSF shall prevent the following types of
1. <u>side-channels within destruction of Subscriber-SCD (FCS_CKM.4)</u>
2. <u>side-channels within Subscriber-SCD transfer (FPT_ITC.1)</u>.

Application note:
The TSF requires the TOE to prevent side-channel attacks against the Subscriber-SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. 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 SCP 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 e.g. the random padding bits in the RSA-signature generated by the same unsuitable pseudo-random number generator as the Subscriber-SCD itself.

5.1.3.7   Subset residual information protection (FDP_RIP.1)

FDP_RIP.1.1   The TSF shall ensure that any previous information content of a resource is made unavailable upon the <u>de-allocation of the resource from</u> the following objects: <u>Subscriber-SCD</u>.

5.1.3.8   Stored data integrity monitoring and action (FDP_SDI.2)

FDP_SDI.2.1   The TSF shall monitor user data stored within the TSC for <u>integrity errors</u> on all objects, based on the following attributes: <u>error detecting code</u>.

FDP_SDI.2.2   Upon detection of a data integrity error, the TSF shall <u>enter the secure blocking state</u>.

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.

5.1.3.9   Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1   The TSF shall enforce the <u>Crypto-SFP</u> to be able to <u>transmit</u> objects in a manner protected from unauthorised disclosure.

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

5.1.4   Identification and authentication (FIA)

5.1.4.1   Authentication failure handling (FIA_AFL.1)

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

FIA_AFL.1.2   When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall <u>block the identity for authentication</u>.

Application note:
The number of authentication failures handling shall be defined with respect to the high strength of the authentication function.

5.1.4.2   User attribute definition (FIA_ATD.1)

FIA_ATD.1.1   The TSF shall maintain the following list of security attributes belonging to individual users: <u>identity and role</u>.

5.1.4.3   Verification of secrets (FIA_SOS.1)

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

Application note:
The quality metric to be defined shall be defined with respect to the high strength of the authentication function and the authentication mechanism to be implemented in the TOE.

5.1.4.4   Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1   The TSF shall allow <u>start-up, self-test (FPT_TST.1), detection of the secure blocking state (FPT_FLS.1), detection of violation of physical integrity (FPT_PHP.2), identification (FIA_UID.1)</u> 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.

5.1.4.5   Timing of identification (FIA_UID.1)

FIA_UID.1.1   The TSF shall allow <u>start-up, self-test (FPT_TST.1), detection of the secure blocking state (FPT_FLS.1), detection of violation of physical integrity (FPT_PHP.2)</u> on behalf of the user to be performed before the user is identified.

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

5.1.5   Security management (FMT)

5.1.5.1   Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1/AUDIT   The TSF shall restrict the ability to <u>determine the behaviour of</u> the function <u>audit (FAU_GEN.1)</u> to <u>Auditor</u>.

FMT_MOF.1.1/PHYS   The TSF shall restrict the ability to <u>determine the behaviour of</u> the function <u>notification of the local user (FPT_PHP.2)</u> to <u>the Crypto-officer or the Auditor</u>.

5.1.5.2   Management of security attributes (FMT_MSA.1/ROLE_CRYPTO)

FMT_MSA.1.1/ ROLE_CRYPTO   The TSF shall enforce the <u>Crypto-SFP</u> to restrict the ability to <u>change default, query, modify and delete</u> the security attributes <u>Role Crypto-officer</u> to <u>Crypto-officer</u>.

5.1.5.3   Management of security attributes (FMT_MSA.1/ROLE_AUDIT)

FMT_MSA.1.1/ ROLE_AUDIT   The TSF shall enforce the <u>Audit-SFP</u> to restrict the ability to <u>query, modify and delete</u> [assignment: *other operations*] the security attributes <u>Role Auditor</u> to <u>Auditor</u>.

5.1.5.4 Secure security attributes (FMT_MSA.2)

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

5.1.5.5 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1   The TSF shall enforce the <u>Crypto-SFP and Audit-SFP</u> to provide <u>restrictive</u> default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2   The TSF shall allow the <u>Auditor and Crypto-officer</u> to specify alternative initial values to override the default values when an object or information is created.

5.1.5.6 Management of TSF data (FMT_MTD.1/ACCESS_CONTROL)

FMT_MTD.1.1/   The TSF shall restrict the ability to <u>query and modify </u>the <u>access control</u>
ACCESS_CONTROL   <u>lists</u> to <u>Crypto-officer</u>.

Application note:
The Crypto-officer is allowed to change the access control lists only within the limits of the defined roles.

5.1.5.7 Management of TSF data (FMT_MTD.1/AUDIT)

FMT_MTD.1.1/   The TSF shall restrict the ability to <u>query</u> the <u>audit data of the TSF</u>
AUDIT   <u>required by FAU_GEN.1</u> to <u>Auditor</u>.

Application note:
The Auditor is allowed to query, export and delete the audit data. The Crypto-officer is allowed to export audit data without deleting them.

5.1.5.8 Management of TSF data (FMT_MTD.1/USER_Crypto)

FMT_MTD.1.1/   The TSF shall restrict the ability to <u>change_default and delete </u>the <u>Identity</u>
USER_CRYPTO   <u>and RAD for user with role attribute Crypto-officer </u>to <u>Crypto-officer</u>.

5.1.5.9 Management of TSF data (FMT_MTD.1/USER_AUDIT)

FMT_MTD.1.1/   The TSF shall restrict the ability to <u>change_default and delete</u> the <u>Identity</u>
USER_AUDIT   <u>and RAD for user with role attribute Auditor</u> to <u>Auditor</u>.

5.1.5.10   Management of TSF data (FMT_MTD.1/RAD)

FMT_MTD.1.1/
RAD

The TSF shall restrict the ability to <u>modify the RAD</u> to <u>user for its own RAD</u>.

5.1.5.11   Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:
1. <u>Definition of the audit function behaviour (FMT_MOF.1.1/AUDIT)</u>
2. <u>Management of the notification of the local user about detected physical attacks (FPT_PHP.2)</u>
3. <u>User management (FMT_MSA.1/ROLE_CRYPTO, FMT_MSA.1/ROLE_AUDIT, FMT_MTD.1/USER_AUDIT, FMT_MTD.1/USER_CRYPTO, FMT_RAD.1)</u>
4. <u>Management of audit data (FMT_MOF.1.1/AUDIT, FMT_MSA.3, FMT_MTD.1/AUDIT).</u>

5.1.5.12   Security roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the roles <u>Crypto-Officer and Auditor.</u>

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 roles shall have the ability to generate Subscriber-SCD/SVD or export Subscriber-SCD/SVD.

5.1.6   Protection of the TOE Security Functions (FPT)

5.1.6.1   Abstract machine testing (FPT_AMT.1)

FPT_AMT.1.1

The TSF shall run a suite of tests <u>at the request of an authorised user</u> to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

5.1.6.2   Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: <u>failures detected by the TSF FPT_AMT.1 and FPT_TST.1</u>.

Refined by adding:

The TSF shall destroy the plaintext Subscriber-SCD and other confidential secret and private keys if failures occur.

5.1.6.3   Notification of physical attack (FPT_PHP.2)

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   The TSF shall monitor the devices and elements and notify <u>local user</u> when physical tampering with the TSF's devices or TSF's elements has occurred.

Refined by adding:

The TSF shall detect physical tampering performed by opening the device or removal of a cover.

Application Note:
The TOE environment should ensure that notification about physical tampering attempts given by the TOE shall be noticed by the CSP security personnel. The TSF configuration for notification of the local user is managed by the Crypto-officer or the Auditor according to FMT_MOF.1. The TOE non-IT environment should ensure that notification about physical tampering attempts given by the TOE shall be noticed by the CSP security personnel.

5.1.6.4   Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1   The TSF shall resist <u>physical tampering by opening the device or removal of a cover</u> to the <u>components which</u>
<u>- generates Subscriber-SCD (FCS_CKM.1)</u>
<u>- stores Subscriber-SCD</u>
<u>- stores other secret or private keys</u>
by responding automatically such that the TSP is not violated.

Refined by adding:
The TSF shall resist the tampering by destruction of plaintext Subscriber-SCD, keys used to establish the trusted channels and other confidential secret and private keys if physical tampering is detected.

Application Note:
The TOE shall protect the confidentiality of the Subscriber-SCD and other secret and private keys in case of physical maintenance or physical tampering. A hard opaque potting material or a strong non-removable enclosure designed such that attempts to remove or penetrate it will have a high probability of causing serious damage to the module. If the detection of opening the device or removal of a cover might not be effective for the switched off device the TOE will destroy the Subscriber-SCD in case of loss of power. The TSF will invoke the TSF required by FCS_CKM.4 to destroy the Subscriber-SCD and all other plaintext secret and private keys. The

destruction of the keys used to establish a trusted channel will prevent the use of an attacked TOE for transfer of Subscriber-SCD until restoring the operational state.

5.1.6.5   Manual recovery (FPT_RCV.1)

FPT_RCV.1.1   After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

5.1.6.6   TSF testing (FPT_TST.1)

FPT_TST.1.1   The TSF shall run a suite of self tests <u>during initial start-up, at the request of the authorised user, at the conditions and at installation and maintenance</u> to demonstrate the correct operation of the TSF.

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

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

Refined by adding:

The TSF shall perform self-tests
1. **Initialisation**
   Extended software/firmware integrity test

2. **Power-Up Tests**
   Software/firmware integrity test
   Internal TSF data integrity test.
   Cryptographic algorithm test.
   Random number generator tests
   Critical functions test.

3. **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.

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 and FCS_RND.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.

5.1.6.7   FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1/ SCD_Export	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SCD_Export	The TSF shall permit <u>the TOE</u> to initiate communication via the trusted channel.
FTP_ITC.1.3/ SCD_Export	The TSF shall initiate communication via the trusted channel for <u>the export of Subscriber-SCD.</u>

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.

FTP_ITC.1.1/ SVD_Export	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/ SVD_Export	The TSF shall permit <u>the TOE</u> to initiate communication via the trusted channel.
FTP_ITC.1.3/ SVD_Export	The TSF shall initiate communication via the trusted channel for <u>the export of Subscriber-SVD.</u>

Application Note:
This trusted channel needs to protect the integrity of the Subscriber-SVD to the CGA or to the Subscriber-SSCD or to both.

5.1.7   Trusted path (FTP)

5.1.7.1   Trusted path (FTP_TRP.1/TOE)

FTP_TRP.1.1/TOE   The TSF shall provide a communication path between itself and <u>local</u> users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2/TOE   The TSF shall permit <u>local users</u> to initiate communication via the trusted path.

FTP_TRP.1.3/TOE   The TSF shall require the use of the trusted path for <u>initial user authentication /FIA_UID.1, FIA_UAU.1) and TSF management (FMT_MSA.1/ROLE_CRYPTO, FMT_MSA.1/ROLE_AUDIT, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1/ACCESS_CONTROL, FMT_MTD.1/AUDIT, FMT_MTD.1/USER_CRYPTO, FMT_MTD.1/USER_AUDIT, FMT_SMR.1).</u>

5.2   TOE Security Assurance Requirements

Table 5.1 Assurance Requirements: EAL 4 augmented

Assurance Class	Assurance Components
ACM	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2
ADO	ADO_DEL.2 ADO_IGS.1
ADV	ADV_FSP.2 ADV_HLD.2 ADV_IMP.2 ADV_LLD.1 ADV_RCR.1 ADV_SPM.1
AGD	AGD_ADM.1 AGD_USR.1
ALC	ALC_DVS.1 ALC_LCD.1 ALC_TAT.1
ATE	ATE_COV.2 ATE_DPT.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_CCA.1 AVA_MSU.2 AVA_SOF.1 AVA_VLA.4

5.2.1 Configuration management (ACM)

5.2.1.1 Partial CM automation (ACM_AUT.1)

ACM_AUT.1.1D   The developer shall use a CM system.

ACM_AUT.1.2D   The developer shall provide a CM plan.

ACM_AUT.1.1C   The CM system shall provide an automated means by which only authorised changes are made to the TOE implementation representation.

ACM_AUT.1.2C   The CM system shall provide an automated means to support the generation of the TOE.

ACM_AUT.1.3C   The CM plan shall describe the automated tools used in the CM system.

ACM_AUT.1.4C   The CM plan shall describe how the automated tools are used in the CM system.

5.2.1.2 Generation support and acceptance procedures (ACM_CAP.4)

ACM_CAP.4.1D   The developer shall provide a reference for the TOE.

ACM_CAP.4.2D   The developer shall use a CM system.

ACM_CAP.4.3D   The developer shall provide CM documentation.

ACM_CAP.4.1C   The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.4.2C   The TOE shall be labelled with its reference.

ACM_CAP.4.3C   The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.
The configuration list shall uniquely identify all configuration items that comprise the TOE.

ACM_CAP.4.4C   The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C   The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.4.6C   The CM system shall uniquely identify all configuration items.

ACM_CAP.4.7C   The CM plan shall describe how the CM system is used.

ACM_CAP.4.8C   The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.4.9C   The CM documentation shall provide evidence that all configuration items

have been and are being effectively maintained under the CM system.

ACM_CAP.4.10C   The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.4.11C   The CM system shall support the generation of the TOE.

ACM_CAP.4.12C   The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.

5.2.1.3   Problem tracking CM coverage (ACM_SCP.2)

ACM_SCP.2.1D   The developer shall provide a list of configuration items for theTOE..

ACM_SCP.2.1C   The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.

5.2.2   Delivery and operation (ADO)

5.2.2.1   Detection of modification (ADO_DEL.2)

ADO_DEL.2.1D   The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.2.2D   The developer shall use the delivery procedures.

ADO_DEL.2.1C   The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.2.2C   The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.

ADO_DEL.2.3C   The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.

5.2.2.2   Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1D   The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C   The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.

5.2.3   Development (ADV)

5.2.3.1   Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.2.1D   The developer shall provide a functional specification.

ADV_FSP.2.1C   The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.2.2C   The functional specification shall be internally consistent.

ADV_FSP.2.3C   The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.

ADV_FSP.2.4C   The functional specification shall completely represent the TSF.

ADV_FSP.2.5C   The functional specification shall include rationale that the TSF is completely represented.

5.2.3.2   Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1D   The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C   The presentation of the high-level design shall be informal.

ADV_HLD.2.2C   The high-level design shall be internally consistent.

ADV_HLD.2.3C   The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C   The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C   The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C   The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C   The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C   The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C   The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

5.2.3.3   Implementation of the TSF (ADV_IMP.2)

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

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

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

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

5.2.3.4   Descriptive low-level design (ADV_LLD.1)

ADV_LLD.1.1D   The developer shall provide the low-level design of the TSF.

ADV_LLD.1.1C   The presentation of the low-level design shall be informal.

ADV_LLD.1.2C   The low-level design shall be internally consistent.

ADV_LLD.1.3C   The low-level design shall describe the TSF in terms of modules.

ADV_LLD.1.4C   The low-level design shall describe the purpose of each module.

ADV_LLD.1.5C   The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.

ADV_LLD.1.6C   The low-level design shall describe how each TSP-enforcing function is provided.

ADV_LLD.1.7C   The low-level design shall identify all interfaces to the modules of the TSF.

ADV_LLD.1.8C   The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.

ADV_LLD.1.9C   The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_LLD.1.10C   The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.

5.2.3.5   Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D   The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C   For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.2.3.6   Informal TOE security policy model (ADV_SPM.1)

ADV_SPM.1.1D   The developer shall provide a TSP model.

ADV_SPM.1.2D   The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.1C   The TSP model shall be informal.

ADV_SPM.1.2C   The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.

ADV_SPM.1.3C   The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.

ADV_SPM.1.4C   The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

5.2.4   Guidance documents (AGD)

5.2.4.1   Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D   The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C   The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C   The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C   The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C   The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C   The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C   The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C   The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C   The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.2.4.2   User guidance (AGD_USR.1)

AGD_USR.1.1D   The developer shall provide user guidance.

AGD_USR.1.1C   The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C   The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C   The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C   The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C   The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C   The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5   Life cycle support (ALC)

5.2.5.1   Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D   The developer shall produce development security documentation.

ALC_DVS.1.1C   The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C   The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.2.5.2   Developer defined life-cycle model (ALC_LCD.1)

ALC_LCD.1.1D   The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.

ALC_LCD.1.2D   The developer shall provide life-cycle definition documentation.

ALC_LCD.1.1C   The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.2C   The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

5.2.5.3   Well-defined development tools (ALC_TAT.1)

ALC_TAT.1.1D   The developer shall identify the development tools being used for the TOE.

ALC_TAT.1.2D   The developer shall document the selected implementation-dependent options of the development tools.

ALC_TAT.1.1C   All development tools used for implementation shall be well-defined.

ALC_TAT.1.2C   The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

ALC_TAT.1.3C   The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

5.2.6   Tests (ATE)

5.2.6.1   Analysis of coverage (ATE_COV.2)

ATE_COV.2.1D   The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C   The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C   The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.2.6.2   Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1D   The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C   The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

5.2.6.3   Functional testing (ATE_FUN.1)

ATE_FUN.1.1D   The developer shall test the TSF and document the results.

ATE_FUN.1.2D   The developer shall provide test documentation.

ATE_FUN.1.1C   The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C   The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C   The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C   The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C   The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.2.6.4   Independent testing - sample (ATE_IND.2)

ATE_IND.2.1D   The developer shall provide the TOE for testing.

ATE_IND.2.1C   The TOE shall be suitable for testing.

ATE_IND.2.2C   The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.7   Vulnerability assessment (AVA)

5.2.7.1   Covert channel analysis (AVA_CCA.1)

AVA_CCA.1.1D   The developer shall conduct a search for covert channels for each information flow control policy.

AVA_CCA.1.2D   The developer shall provide covert channel analysis documentation.

AVA_CCA.1.1C   The analysis documentation shall identify covert channels and estimate their capacity.

AVA_CCA.1.2C   The analysis documentation shall describe the procedures used for

determining the existence of covert channels, and the information needed to carry out the covert channel analysis.

AVA_CCA.1.3C   The analysis documentation shall describe all assumptions made during the covert channel analysis.

AVA_CCA.1.4C   The analysis documentation shall describe the method used for estimating channel capacity, based on worst case scenarios.

AVA_CCA.1.5C   The analysis documentation shall describe the worst case exploitation scenario for each identified covert channel.

5.2.7.2 Validation of analysis (AVA_MSU.2)

AVA_MSU.2.1D   The developer shall provide guidance documentation.

AVA_MSU.2.2D   The developer shall document an analysis of the guidance documentation.

AVA_MSU.2.1C   The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.2.2C   The guidance documentation shall be complete, clear, consistent and reasonable.

AVA_MSU.2.3C   The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.2.4C   The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.2.5C   The analysis documentation shall demonstrate that the guidance documentation is complete.

5.2.7.3 Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1D   The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C   For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C   For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.2.7.4   Highly resistant (AVA_VLA.4)

AVA_VLA.4.1D   The developer shall perform a vulnerability analysis.

AVA_VLA.4.2D   The developer shall provide vulnerability analysis documentation.

AVA_VLA.4.1C   The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which a user can violate the TSP.

AVA_VLA.4.2C   The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.

AVA_VLA.4.3C   The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.4.4C   The vulnerability analysis documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

AVA_VLA.4.5C   The vulnerability analysis documentation shall show that the search for vulnerabilities is systematic.

AVA_VLA.4.6C   The vulnerability analysis documentation shall provide a justification that the analysis completely addresses the TOE deliverables.

5.3   Security Requirements for the IT Environment

5.3.1   Security audit (FAU)

5.3.1.1   Audit review (FAU_SAR.1)

FAU_SAR.1.1 /ENV   The IT environment shall provide <u>System auditor of the CSP</u> with the capability to read <u>all audit information produced by the TOE</u> from the audit records.

FAU_SAR.1.2 /ENV   The IT environment shall provide the audit records in a manner suitable for the user to interpret the information.

5.3.1.2   Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 /ENV   The IT environment shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 /ENV   The IT environment shall be able to <u>prevent</u> modifications to the audit records.

5.3.1.3   Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/
SCD Import

The IT environment shall perform <u>encryption</u> 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*].

Application note:
The TSF of the Subscriber-SSCD will be used for the import of the Subscriber-SCD via a trusted channel (see FTP_ITC.1/SCD_Export and FPT_ITC.1/SCD_Import) to ensure the confidentiality.

5.3.2   Trusted path/channels (FTP)

5.3.2.1   Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1/
SCD Import

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

FTP_ITC.1.2/
SCD Import

The IT environment shall permit <u>the remote trusted IT product</u> to initiate communication via the trusted channel.

FTP_ITC.1.3/
SCD Import

The IT environment shall initiate communication via the trusted channel for <u>Subscriber-SCD import</u>.

Application notes
The trusted channels for Subscriber-SCD import should be established by means of cryptographic mechanisms.

FTP_ITC.1.1/
SVD Import

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

FTP_ITC.1.2/
SVD Import

The IT environment shall permit <u>the remote trusted IT product</u> to initiate communication via the trusted channel.

FTP_ITC.1.3/
SVD Import

The IT environment shall initiate communication via the trusted channel for <u>SVD import</u>.

Application notes
The SVD may be imported by the certification-generation application or by the Subscriber-SSCD for storing and future export to a certification-generation application.

5.3.2.2   Trusted path (FTP_TRP.1)

FTP_TRP.1.1 /CLIENT   The IT environment shall provide a communication path between itself and <u>local</u> users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 /CLIENT   The IT environment shall permit <u>local users</u> to initiate communication via the trusted path.

FTP_TRP.1.3 /CLIENT   The IT environment shall require the use of the trusted path for <u>communication with TOE for identification, authentication and management</u>.

5.3.3   Non-IT requirements

RE.ENV_Personnel   *Personnel security measures*

The CSP shall define the obligations and the services of management and operation roles for the TOE. The CSP shall inform and train the personnel for their roles. The CSP shall inform the personnel using the TOE about their civil, financial and legal responsibilities.

RE.ENV_Protect_Access   *Physical protection of the TOE*

The CSP shall establish physical and organisational security measures to protect the TOE against theft and modification of TOE hardware, firmware and software. These measures shall restrict the access to the TOE and protected assets to authorised persons. If the TOE detects and notifies about physical tampering the local users shall inform the CSP security staff. The TOE shall not be used until the physical integrity of the TOE is established.

RE.ENV_Secure_Init   *Secure initialisation of the TOE*

The CSP shall define and apply procedures and controls in the TOE environment which allow to securely set-up and initialise the TOE for the generation of Subscriber-SCD. This includes

(1) dual control for secure installation and initialisation of the TOE in the CSP,

(2) the Subscriber-SCD / Subscriber-SVD pair generation,

(3) the export of the Subscriber-SCD and Subscriber-SVD by the TOE and the securing the authenticity of the Subscriber-SVD,

(4) the secure initial configuration of the TSF data user's identity, roles and user authentication information.

RE.ENV_Secure_Oper   *Secure operation of the TOE*

The CSP shall define and apply procedures and controls in the TOE environment which allow operating the TOE within a CA system in compliance with the requirements of the EU directive, the Qualified Certificates Policy for the issued certificates, the secure operation of the client application and the TOE guidance.

The TOE user shall ensure that notification about physical tampering attempts given by the TOE will be noticed by the CSP security personnel.

6 Rationale

6.1 Security Objectives Rationale

6.1.1 Security Objectives Coverage

Table 6-1 Security Environment to Security Objective Mapping

	T.Bad_SW	T.Subscriber-SCD_Derive	T.Subscriber-SCD_Disclose	T.Malfunction	T.Management	T.Misuse	T.Phys_Manipul	T.Subscriber-SCD_Copy	T.SVD_Forgery	T.Insecure_Init	T.Insecure_Oper	A.Audit_Support	A.Human_interface	P.Algorithms
O.Audit_CM	x			x	x	x				x				
O.Subs_SCD_Secure		x	x											x
O.Check_Operation				x										
O.Control_Services	x			x	x					x				
O.Detect_Attack							x							
O.Error_secure				x			x							
O.SCD_Transfer			x					x						
O.SVD_Transfer									x					
O.User_authentication	x				x									
O.ENV_Audit												x		
O.ENV_Human_interface													x	
O.ENV_Personnel	x				x					x	x	x		
O.ENV_Protect_Access							x				x			
O.ENV_Secure_Init										x				
O.ENV_Secure_Oper		x	x								x			
O.ENV_SCD_Transfer			x					x						
O.ENV_SVD_Transfer									x					

6.1.2   Security Objectives Sufficiency

6.1.2.1   Policies and Security Objective Sufficiency

P.Algorithms (Use of Approved Algorithms and Algorithm Parameter) addresses the problem to use only algorithms and algorithm parameter defined as acceptable for being used for Subscriber-SCD/SVD pair generation within the key generation process. Where confidentiality protection is required such as for the transfer of Subscriber-SCD to the user devices, only algorithms and algorithm parameters defined as acceptable for that purpose shall be used. **O.Subs-SCD_Secure** (Secure Subscriber-SCD Generation and Management) requires the TOE to implement secure cryptographic algorithms and parameters for the Subscriber-SCD/SVD pair generation chosen from [5].ensures the confidentiality and integrity of the Subscriber-SCD as long as they are under the control of the TOE.

6.1.2.2   Threats and Security Objective Sufficiency

T.Bad_SW (Malicious Software during the Lifetime of the TOE) deals with the threat that the TOE provides the ability to load new software or software updates or to modify software when it is in operation and that this function can be misused to load malicious software. **O.Audit_CM** (Audit record generation and export) shall audit the TOE initialisation, start-up and self test at the condition installation and maintenance that can be used to detect and prevent misuse. **O.Control_Services** (Management and control of TOE services) forces the TOE to restrict the access to its services, depending on the user role, to those services explicitly assigned to this role. **O.User_authentication** (Authentication of Users interacting with the TOE) enables the TOE to identify and authenticate the users acting with a defined role, before allowing any access to TOE as required for the O.Control_Services. The objective for the environment **O.ENV_Personnel** (Reliable Personnel) ensures 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.

T.Subscriber-SCD_Derive (Deriving All or Parts of Subscriber-SCD) addresses the ability to derive all or parts of Subscriber-SCD in any way (including the legitimate use of the TOE services and using knowledge about the key generation process). **O.Subs-SCD_Secure** (Secure Subscriber-SCD Generation and Management) ensures cryptographic secure Subscriber-SCD/SVD pair generation and transfer to the subscriber SSCD. This includes protection against disclosing completely or partly the Subscriber-SCD in clear through any physical or logical TOE interface. Also the TOE shall not use any Subscriber-SCD for signature creation. **O.ENV_Secure_Oper** (Secure Operating Procedures) defines procedures and controls in the TOE environment that allow operating the TOE within a CA system in compliance with the requirements of the EU directive and the Policy for certification authorities issuing qualified certificates.

T.Subscriber-SCD_Disclose (Disclosing All or Part of Subscriber-SCD) addresses the threat of direct disclosure of Subscriber-SCD or part of it. This includes any way of disclosing all or part of the Subscriber-SCD generated by the TOE by any data intentionally exported by the TOE or over any physical or logical TOE interface as addressed by **O.Subs-SCD_Secure**. The **O.SCD_Transfer** (Secure transfer of Subscriber-SCD to the SSCD) provides that the TOE ensures the confidentiality of the Subscriber-SCD transferred from the TOE to a SSCD via a trusted channel. The Subscriber-SCD will be deleted by the TOE after use (i.e. exported to the SSCD). Note that the SSCD receiving the exported Subscriber-SCD will protect the Subscriber-

SCD against discloser according to **O.ENV_SCD_Transfer**. **O.ENV_Secure_Oper** (Secure Operating Procedures) defines procedures and controls in the TOE environment that allow operating the TOE within a CA system in compliance with the requirements of the EU directive and the Policy for certification authorities issuing qualified certificates.

T.Malfunction (Malfunction of the TOE) deals with the threat that internal malfunction of TOE functions may result in the generation of Subscriber-SCD of low quality or invalid Subscriber-SCD, misuse of TOE services, disclosure or distortion of Subscriber-SCD or denial of service for authorised users. A failure of such a critical hardware component could result in the disclosure or distortion of secret keys or the ability to misuse services of the TOE. **O.Check_Operation** (Check for Correct Operation) ensures that TOE shall perform regular checks to verify that its components operate correctly. **O.Error_secure** (Secure state in case of error) ensures that the TOE shall enter a secure state whenever it detects an error. The secure state shall prevent the loss of confidentiality of the Subscriber-SCD. **O.Audit_CM** (Audit record generation and export) ensures audit information about unsuccessful self test operations detecting TOE internal errors.

T.Management (Misuse of Management) addresses the threat that assets are revealed in TOE initialisation, start-up and operation due to attack during initialisation and by CSP personnel using TOE services. **O.Audit_CM** (Audit record generation and export) ensures the audit of TOE initialisation, TOE start-up, modification of TOE management data, handling new users or roles and reading and deleting audit trail records. **O.Control_Services** (Management and control of TOE services) provides the TOE to restrict the access to its services, depending on the user role, to those services explicitly assigned to this role. Assignment of services to roles shall be either done by explicit action of a system administrator or by default. Roles may also be predefined in the production or initialisation phase. **O.User_authentication** (Authentication of Users interacting with the TOE) enables the TOE to identify and authenticate the users acting with a defined role, before allowing any access to TOE protected assets. Identification and authentication may also be user-based or may be user-based for defined roles. At least for the roles Administrator and Crypto-officer user based authentication is required. Additional **O.ENV_Personnel** (Reliable Personnel) ensures that the personnel using the TOE services will be aware of civil, financial and legal responsibilities, as well as the obligations they have to face, depending on their role.

T.Misuse (Misuse of Subscriber-SCD/SVD pair generation function) addresses the threat that an attacker misuses the TOE for generation of Subscriber-SCD/SVD pairs. This may result in Subscriber-SCD/SVD pairs that are used without proper authorization. **O.Control_Services** (Management and control of TOE services) provides the TOE to restrict the access to its services, depending on the user role, to those services explicitly assigned to this role. The **O.Audit_CM** (Audit record generation and export) shall audit the generation and destruction of Subscriber-SCD.

T.Phys_Manipul (Physical Manipulation of the TOE) deals with an attacker which may try to physically manipulate the TOE with the intent to derive all or part of the Subscriber-SCD or to misuse services of the TOE. **O.Detect_Attack** (Detection of Physical Attacks) guarantees that the TOE detects attempts of physical tampering and securely destroy the Subscriber-SCD in this case. **O.Error_secure** (Secure state in case of error) provides the TOE to enter a secure state whenever it detects an error. The secure state shall prevent the loss of confidentiality of the Subscriber-SCD. Note that **O.ENV_Protect_Access** (Prevention of Unauthorised Physical Access) adds physical, logical and organisational protection measures to protect the TOE.

T.Subscriber-SCD_Copy (Uniqueness of Subscriber-SCD) handles the threat that a Subscriber-SCD generated by the TOE may be transferred to more than one SSCD which may result in the possibility for one owner of such a SSCD to forge the signature of the owner of another SSCD that uses the same Subscriber-SCD. **O.SCD_Transfer** (Secure transfer of Subscriber-SCD to the SSCD) and the **O.ENV_SCD_Transfer** (Secure import of Subscriber-SCD to SSCD) provides that the Subscriber-SCD is transmitted via secure channel to the SSCD ensuring the confidentiality of the Subscriber-SCD. Moreover the TOE will delete the Subscriber-SCD whenever it is exported from that TOE.

T.SVD_Forgery (Forgery of the signature-verification data) addresses the forgery of the SVD during transmission between the TOE and the CGA or the SSCD if it stores the SVD for later transmission to the CGA. The **O.SVD_Transfer** ans the **O.ENV_SVD_Transfer** requires the TOE and the IT environment (CGA or SSCD) together to ensure the integrity of the SVD.

T.Insecure_Init (Insecure Initialisation of the TOE) handles the threat that the TOE may be initialised in an insecure environment, by unauthorised personnel or without using adequate organisational controls. **O.Audit_CM** (Audit record generation and export) 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 initialisation process. The **O.Control_Services** (Management and control of 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. **O.ENV_Personnel** (Reliable Personnel) provides 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. **O.ENV_Secure_Init** (Secure Initialisation Procedures) deals with procedures and controls defined and applied in the TOE environment that allow to securely set-up and initialise the TOE for the generation of signatures for qualified certificates or certificate status information.

T.Insecure_Oper (Insecure Operation of the TOE) deals with the threat that the TOE may be operated in an insecure way not detectable by the TOE itself. This includes the use and operation of the TOE within another environment than the intended one (e. g. the TOE may be connected to a hostile system). **O.ENV_Personnel** (Reliable Personnel) ensures 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 includes training on correct usage of the TOE. **O.ENV_Protect_Access** (Prevention of Unauthorised Physical Access) provides the TOE to be protected by physical and logical protection measures, in order to prevent any TOE theft or modification, as well as any protected assets disclosure. Those measures shall especially restrict the TOE usage and the access to its assets to authorised persons only. The entire contents of a cryptographic module, including hardware, firmware, software and data shall be protected. **O.ENV_Secure_Oper** (Secure Operating Procedures) deals with procedures and controls definition in the TOE environment that allow operating the TOE within a CA system in compliance with the requirements of the EU directive and the Policy for certification authorities issuing qualified certificates.

6.1.2.3   Assumptions and Security Objective Sufficiency

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 **O.ENV_Audit** (Audit review) as the environment provides a review of the audit trail recorded by the TOE. **O.ENV_Personnel** (Reliable Personnel) enhances the fulfilment of this necessity while 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.Human_Interface (Interface with Human Users) addresses the assumption that the TOE does not have a human interface but the client application will provide an appropriate interface and communication path between human users and the TOE for authentication and management services. **O.ENV_Human_Interface** (Reliable Human Interface) ensures that the client application will ensure the confidentiality and integrity of the data transferred between the TOE and the human user.

6.2   Security Requirements Rationale

6.2.1   Security Requirement Coverage

Table 6-2 Functional Requirement to Security Objective Mapping

	O.Audit_CM	O.Subs_SCD_Secure	O.Check_Operation	O.Control_Services	O.Detect_Attack	O.Error_Secure	O.SCD_Transfer	O.SVD_Transfer	O.User_Authentication	O.ENV_Audit	O.ENV_Human_Interface	O.ENV_Personnel	O.ENV_Protect_Access	O.ENV_Secure_Init	O.ENV_Secure_Oper	O.ENV_SCD_Transfer	O.ENV_SVD_Transfer
FAU_GEN.1	x																
FAU_GEN.2	x																
FAU_STG.2/TOE	x																
FCS_CKM.1		x															
FCS_CKM.4		x															
FCS_COP.1/ SCD Export		x					x										
FCS_RND.1		x															
FDP_ACC.1/AUDIT	x			x													
FDP_ACC.1/CRYPTO				x													
FDP_ACF.1/AUDIT	x			x													
FDP_ACF.1/CRYPTO				x													
FDP_IFC.1		x															
FDP_IFF.4		x															
FDP_RIP.1		x															

	O.Audit_CM	O.Subs_SCD_Secure	O.Check_Operation	O.Control_Services	O.Detect_Attack	O.Error_Secure	O.SCD_Transfer	O.SVD_Transfer	O.User_Authentication	O.ENV_Audit	O.ENV_Human_Interface	O.ENV_Personnel	O.ENV_Protect_Access	O.ENV_Secure_Init	O.ENV_Secure_Oper	O.ENV_SCD_Transfer	O.ENV_SVD_Transfer
FDP_SDI.2		x															
FDP_UCT.1		x					x										
FIA_AFL.1									x								
FIA_ATD.1									x								
FIA_SOS.1									x								
FIA_UAU.1									x								
FIA_UID.1									x								
FMT_MOF.1/AUDIT	x			x													
FMT_MOF.1/PHYS				x	x												
FMT_MSA.1/ROLE_AUDIT	x			x													
FMT_MSA.1/ROLE_CRYPTO				x													
FMT_MSA.2				x													
FMT_MSA.3				x													
FMT_MTD.1/USER_AUDIT	x			x					x								
FMT_MTD.1/USER_CRYPTO				x					x								
FMT_MTD.1/ACCESS_CONTROL				x													
FMT_MTD.1/AUDIT	x			x													
FMT_MTD.1/RAD				x					x								
FMT_SMF.1	x			x	x				x								
FMT_SMR.1				x													
FPT_AMT.1			x			x											
FPT_FLS.1						x											
FPT_PHP.2					x												

	O.Audit_CM	O.Subs_SCD_Secure	O.Check_Operation	O.Control_Services	O.Detect_Attack	O.Error_Secure	O.SCD_Transfer	O.SVD_Transfer	O.User_Authentication	O.ENV_Audit	O.ENV_Human_Interface	O.ENV_Personnel	O.ENV_Protect_Access	O.ENV_Secure_Init	O.ENV_Secure_Oper	O.ENV_SCD_Transfer	O.ENV_SVD_Transfer
FPT_PHP.3					x												
FPT_RCV.1						x											
FPT_TST.1			x		x	x											
FTP_ITC.1/ SCD_Export							x										
FTP_ITC.1/ SVD_Export								x									
FTP_TRP.1/TOE									x								
FAU_SAR.1/ENV										x							
FAU_STG.1/ENV										x							
FCS_COP.1/ SCD Import																x	
FTP_ITC.1/ SCD_Import																x	
FTP_ITC.1/ SVD_Import																	x
FTP_TRP.1/CLIENT											x						
RE.ENV_Personnel												x					
RE.ENV_Protect_Acce													x				
RE.ENV_Secure_Init														x			
RE.ENV_Secure_Oper															x		

The security assurance are not indicated in the table but handled in the next section and in section 6.6 "Rationale for Assurance Level 4 Augmented".

6.2.2   Security Requirements Sufficiency

6.2.2.1   TOE Security Requirements Sufficiency

O.Audit_CM (Audit record generation and export) addresses the generation and protection of audit data by the TOE. The audit generation is implemented by the SFR **FAU_GEN.1** (Audit data generation) and **FAU_GEN.2** (User identity association) with the audit events matching the list in O.Audit_CM. The TOE stores the audit data according to the SFR **FAU_STG.2/TOE** (Guarantees of audit data availability) until the audit trail is exported upon request of the Auditor or the Crypto-officer under control of the SFR **FDP_ACC.1/AUDIT** (Subset access control) and **FDP_ACF.1/AUDIT** (Security attribute based access control). The SFR **FMT_MOF.1/AUDIT** (Management of security functions behaviour) and **FMT_MTD.1/AUDIT** (Management of TSF data) specify and **FMT_SMF.1** (Specification of Management Functions) lists the requirements of the management of the audit function. The behaviour of the audit function is managed by the Auditor role which is separated from Crypto-officer role by management functions **FMT_MSA.1/ROLE_AUDIT** and **FMT_MTD.1/USER_AUDIT**.

O.Subs-SCD_Secure (Secure Subscriber-SCD Generation and Management) addresses the confidentiality and integrity of the Subscriber-SCD. The cryptographic security of the Subscriber-SCD is implemented by the SFR **FCS_CKM.1** (Cryptographic key generation) and **FCS_RND.1** (Quality metrics for random numbers). The SFR **FCS_CKM.4** (Cryptographic key destruction) ensures that the key is actively deleted after export, furthermore the SFR **FDP_RIP.1** (Subset residual information protection) prevents the illicit availability of previous information content. For protection against integrity errors an error detecting code is provided by the SFR **FDP_SDI.2** (Stored data integrity monitoring and action). In case of an error occurrence a secure blocking state will be entered. The SFR **FCS_COP.1** protects cryptographically the Subscriber-SCD during the transfer from the TOE into the SSCD. The SFR **FDP_IFC.1** (Subset information flow control) and **FDP_IFF.4** (Partial elimination of illicit information flows) requires TSF to prevent illicit information flow about the Subscriber-SCD through side-channels in the signatures. The SAR **AVA_CCA.1** (Covert channel analysis) and **AVA_VLA.4** (Highly resistant) requires covert-channel analysis and a systematic and complete vulnerability analysis considering high attack potential. That is because the generation of the Subscriber-SCD is the most important and critical service of the TOE.

O.Check_Operation (Check for Correct Operation) addresses regular checks to verify that its components operate correctly. This security objective is implemented in the TOE by the SFR **FPT_AMT.1** (abstract machine testing) and **FPT_TST.1** (TSF testing). If these tests detect an error the TOE will transit into a secure state (see O.Error_secure) and prevent the normal operation.

O.Control_Services (Management and control of TOE services) addresses the access control to TOE services and its management. The access control is implemented in the TOE by: **FDP_ACC.1/CRYPTO** (Subset access control) and **FDP_ACF.1/CRYPTO** (Security attribute based access control) for the cryptographic functions (Crypto-SFP), **FDP_ACC.1/AUDIT** (Subset access control) and **FDP_ACF.1/AUDIT** (Security attribute based access control) for the audit function (Audit-SFP), with the roles Auditor and Crypto-officer as defined by the SFR **FMT_SMR.1** (Security roles). The SFR **FMT_MOF.1/AUDIT** (Management of security functions behaviour) and **FMT_MOF.1/PHYS** (Management of security functions behaviour) assign separately to Auditor and Crypto-officer the management of the TSF behaviour. The roles Auditor and Crypto-officer are separated by SFR **FMT_MTD.1/ACCESS_CONTROL**

(Management of TSF data), **FMT_MTD.1/AUDIT** (Management of TSF data). The SFR for management of TSF data **FMT_MTD.1/USER_AUDIT**, **FMT_MTD.1/USER_CRYPTO** and **FMT_MTD.1/RAD** ensure that the RAD may be modified by the RAD-owner and may be deleted by a in the same role only. Note that the user management is addressed by O.User_authentication. The SFR **FMT_MSA.1/ROLE_AUDIT** (Management of security attributes), **FMT_MSA.1/ROLE_CRYPTO** (Management of security attributes), **FMT_MSA.2** (Secure security attributes), **FMT_MSA.3** (Static attribute initialisation) restrict the ability to modify the default values and to delete the security attributes which may be changed respectively by the Crypto-officer and Auditor. The SFR **FMT_SMF.1** (Specification of Management functions) list these management functions.

O.Detect_Attack (Detection of Physical Attacks) addresses the detection of physical tampering attempts and the secure destruction of the Subscriber-SCD if such attempts are detected. The SFR **FPT_PHP.2** (Notification of physical attack) implements notification of and **FPT_PHP.3** (Resistance to physical attack). The behaviour of the notification of the local user in case of a detected attack (see FPT_PHP.2) is managed according to **FMT_MOF.1/PHYS** (Management of security functions behaviour). This management SFR is also listed in **FMT_SMF.1** (Specification of Management functions). The refinement of FPT_PHP.3 limits the tamper scenarios to opening the device or removal of a cover. This limitation is reasonable because **RE.ENV_Protect_Access** requires CSP security measures for physical protection of the TOE. The SFR **FPT_TST.1** (TSF testing) verifies the integrity and authenticity of the TSF executable code at installation, maintenance and initialisation to prevent malicious software running on the TOE. The assurance requirements in the development environment, especial **ACM_CAP.4** (Generation support and acceptance procedures), **ADO_DEL.2** (Detection of modification), **ADO_IGS.1** (Installation, generation, and start-up procedures), **ALC_DVS.1** (Identification of security measures) and **ALC_LCD.1** (Developer defined life-cycle model), prevent that malicious code is installed or hardware is manipulated during the development, production or delivery of the TOE.

O.Error_Secure (Secure state in case of error) addresses a secure state and protection of Subscriber-SCD confidentiality whenever the TOE detects an error. The SFR **FPT_AMT.1** (Abstract machine testing) and **FPT_TST.1** (TSF testing) require tests for error detection and the SFR **FPT_FLS.1** (Failure with preservation of secure state) requires preservation of a secure state when errors are detected. The TSF shall destroy the plaintext Subscriber-SCD and other confidential secret and private keys if failures occur. The SFR **FPT_RCV.1** (Manual recovery) requires a maintenance mode where the ability to return the TOE to a secure state is provided.

O.SCD_Transfer (Secure export of Subscriber-SCD to the SSCD) is provided by **FDP_UCT.1** (Basic data exchange confidentiality) that ensures that the transmission provides the maintenance of confidentiality. This confidentiality is established within the security function **FTP_ITC.1** (Inter-TSF trusted channel) by means of encryption defined by **FCS_COP.1/SCD_Export** (Cryptographic operation) of the TOE. Note that the O.ENV_SCD_Transfer ensures by the FCS_COP.1/SCD_Import (Cryptographic operation) the cryptographic support in the Subscriber-SSCD in the TOE environment.

O.SVD_Transfer (Secure export of SVD to CGA or SSCD) requires to ensure the integrity of the SVD exported to CGA or to the Subscriber-SSCD. This protection is provided by means of a trusted channel by the TOE by **FTP_ITC.1/SVD_Export** (Inter-TSF trusted channel). Note that

this trusted channel is supported in the CGA and the Subscriber-SSCD by O.ENV_SVD_Import which is implemented by TP_ITC.1/SVD_Import (Inter-TSF trusted channel).

O.User_Authentication (Authentication of Users interacting with the TOE) addresses the identification and authentication of the users before having any access to TOE protected assets. The SFR require timing identification by **FIA_UID.1** (Timing of identification) and timing authentication by **FIA_UAU.1** (Timing of authentication). The following actions are allowed on behalf of the user to be performed before the user is authenticated: start-up, identification (FIA_UID.1), self-test (FPT_TST.1), detection of the secure blocking state (FPT_FLS.1) and detection of violation of physical integrity (FPT_PHP.2). Therefore these actions support the TOE protection and do not allow any access to the TOE protected assets. The SFR **FIA_ATD.1** (User attribute definition) defines the security attributes for identity based authentication. The SFR **FIA_SOS.1** (Verification of secrets) ensures the verification of the quality of the secret used for authentication. The SFR **FIA_AFL.1** (Authentication failure handling) protects the RAD against guessing. The TSF **FTP_TRP.1/TOE** (Trusted path) supports the confidentiality of the VAD and RAD (for changing authentication data) during transmission between the TOE and the client application. The SFR for the Management of TSF data **FMT_MTD.1/USER_AUDIT**, **FMT_MTD.1/USER_CRYPTO** and **FMT_MTD.1/RAD** manage the authentication data as listed by **FMT_SMF.1** (Specification of Management Functions). These SFR ensure that the RAD may be modified by the RAD-owner and may be deleted by a in the same role only.

6.2.2.2   TOE Environment Security Requirements Sufficiency

O.ENV_Audit (Audit review) addresses the review of the audit trail recorded by the TOE. The audit review of TOE's audit data is implemented in the IT environment by the SFR **FAU_SAR.1/ENV** (Audit review). Because the TOE implements access control on reading the TOE's audit trail only the SFR **FAU_STG.1/ENV** (Guarantees of audit data availability) ensures the availability of the TOE audit trail and prevents the modification of the TOE audit trail outside the TOE.

O.ENV_Human_Interface (Reliable human interface) addresses the confidentiality and integrity of the data transferred between the TOE and the human user if the client application provides a human interface and a communication path between human users and the TOE. In this case the client application will implement the trusted path according to SFR **FTP_TRP.1/CLIENT** (Trusted path) for transmission of authentication and management data of the human user to the TOE.

O.ENV_Personnel (Reliable Personnel) addresses the awareness of civil, financial and legal responsibilities, as well as the obligations the CSP personnel have to face, depending on their role. The **RE.ENV_Personnel** implements the definition of the obligations, the services and the roles of the TOE users. The CSP shall inform about their civil, financial and legal responsibilities and train the personnel for their roles.

O.ENV_Protect_Access (Prevention of Unauthorised Physical Access) addresses the protection of the TOE by physical and logical protection measures, in order to prevent any TOE theft or modification, as well as any protected assets disclosure. **RE.ENV_Protect_Access** (Physical protection of the TOE) ensures this protection by establishing physical and organisational measures, especially restricting the TOE usage and the access to its assets to

authorised persons only. Furthermore it ensures that the entire contents of a cryptographic module, including hardware, firmware, software and data shall be protected and TOE shall not be used until the physical integrity of the TOE is established.

O.ENV_Secure_Init (Secure Initialisation Procedures) addresses secure set-up and initialisation the TOE for the CSP services. The **RE.ENV_Secure_Init** implements the definition and application of procedures and controls set-up the TOE for the secure generation of Subscriber-SCD and initialisation as well as the initial configuration of other TSF data like roles, users and user authentication information.

O.ENV_Secure_Oper (Secure Operating Procedures) addresses the procedures and controls in the TOE environment to operate the TOE within a CA system in compliance with the requirements of the EU directive and the Policy for certification authorities issuing qualified certificates. The **RE.ENV_Secure_Oper** requires the implementation of such procedures and controls and the observance of the TOE guidance. Furthermore it ensures that the TOE user notification about physical tampering attempts, given by the TOE, will be noticed by the CSP security personnel.

O.ENV_SCD_Transfer (Secure transfer of Subscriber-SCD to SSCD) shall ensure the confidentiality and the integrity of the Subscriber-SCD transferred from the TOE to the SSCD Type2. This function is provided by the SFR **FTP_ITC.1/SCD_Import** (Inter-TSF trusted channel) by cryptographic means as required by **FCS_COP.1/SCD_Import** (Cryptographic operation). Note that these SFR are necessary for interaction with the TSF required by FTP_ITC.1 (Inter-TSF trusted channel) and FCS_COP.1/SCD_Export (Cryptographic operation) for the TOE.

O.ENV_SVD_Transfer (Secure transfer of SVD to SSCD or CGA) shall ensure the integrity of the SVD transferred from the TOE to the CGA or the Subscriber-SSCD or both. In those cases the CGA or the SSCD shall provide the trusted channel provided by the SFR **FTP_ITC.1/SVD_Import** (Inter-TSF trusted channel) to interact with the trusted channel required by FPT_ITC.1/SVD_Export for the TOE.

6.3 Dependency Rationale

6.3.1 Functional and Assurance Requirements Dependencies

Table 6-3 TOE Security Functional Requirements Dependencies

Security Functional Requirements		
Component	Dependency	Remark
FAU_GEN.1	FPT_STM.1	not fulfilled, see refinement to FAU_GEN.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	fulfilled
FAU_STG.2/TOE	FAU_GEN.1	fulfilled
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4 FMT_MSA.2	The TOE generates, exports and delete the Subcriber-SCD but does

Security Functional Requirements		
Component	Dependency	Remark
		not use them for signing. Therefore FCS_COP.1 for the Subcriber-SCD is not included. FCS_CKM.4 and FMT_MSA.2 is included in the PP
FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1 FMT_MSA.2	FCS_CKM.1 and FMT_MSA.2 are included.
FCS_COP.1/SCD_Export	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FCS_CKM.4 included, not fulfilled for [FDP_ITC.1 or FCS_CKM.1] and FMT_MSA.2, see rationale below
FCS_RND.1	FPT_TST.1	fulfilled
FDP_ACC.1/CRYPTO	FDP_ACF.1/CRYPTO	fulfilled
FDP_ACC.1/AUDIT	FDP_ACF.1/AUDIT	fulfilled
FDP_ACF.1	FDP_ACC.1/CRYPTO FMT_MSA.3	fulfilled
FDP_ACF.1/AUDIT	FDP_ACC.1/AUDIT FMT_MSA.3	fulfilled
FDP_IFC.1	FDP_IFF.1	not fulfilled, information flow policy is implemented by FDP_IFF.4
FDP_IFF.4	AVA_CCA.1, FDP_IFC.1	fulfilled
FDP_RIP.1	(no dependencies)	
FDP_SDI.2	(no dependencies)	
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1 FDP_ACC.1 or FDP_IFC.1	FTP_ITC.1 and FDP_ACC.1/CRYPTO, fulfilled
FIA_AFL.1	FIA_UAU.1	fulfilled
FIA_ATD.1	(no dependencies)	
FIA_SOS.1	(no dependencies)	
FIA_UAU.1	FIA_UID.1	fulfilled
FIA_UID.1	(no dependencies)	
FMT_MOF.1.1/AUDIT	FMT_SMF.1, FMT_SMR.1	fulfilled
FMT_MOF.1.1/PHYS	FMT_SMF.1, FMT_SMR.1	fulfilled
FMT_MSA.1/ROLE_CRYPTO	FDP_ACC.1/CRYPTO or FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	FDP_ACC.1/CRYPTO included, fulfilled
FMT_MSA.1/ROLE_AUDIT	FDP_ACC.1/AUDIT or FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	FDP_ACC.1/AUDIT included, fulfilled
FMT_MSA.2	ADV_SPM.1 FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1	FDP_ACC.1/CRYPTO included, fulfilled

Security Functional Requirements		
Component	Dependency	Remark
	FMT_SMR.1	
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	fulfilled
FMT_MTD.1/ACCESS_CONTROL	FMT_SMF.1, FMT_SMR.1	fulfilled
FMT_MTD.1/AUDIT	FMT_SMF.1, FMT_SMR.1	fulfilled
FMT_MTD.1/USER_CRYPTO	FMT_SMF.1, FMT_SMR.1	fulfilled
FMT_MTD.1/USER_AUDIT	FMT_SMF.1, FMT_SMR.1	fulfilled
FMT_SMF.1	(no dependencies)	
FMT_SMR.1	FIA_UID.1	fulfilled
FPT_AMT.1	(no dependencies)	
FPT_FLS.1	ADV_SPM.1	fulfilled
FPT_PHP.2	FMT_MOF.1/PHYS	fulfilled
FPT_PHP.3	(no dependencies)	
FPT_RCV.1	FPT_TST.1, AGD_ADM.1, ADV_SPM.1	fulfilled
FPT_TST.1	FPT_AMT.1	fulfilled
FTP_ITC.1/SCD_Export	(no dependencies)	
FTP_ITC.1/SVD_Export	(no dependencies)	
FTP_TRP.1/TOE	(no dependencies)	

Table 6-4 Security Assurance Requirements Dependencies

Security Assurance Requirements		
Component	Dependency	Remark
ACM_AUT.1	ACM_CAP.3	covered by ACM_CAP.4
ACM_CAP.4	ACM_SCP.1 ALC_DVS.1	covered by ACM_SCP.2
ACM_SCP.2	ACM_CAP.3	covered by ACM_CAP.4
ADO_DEL.2	ACM_CAP.3	covered by ACM_CAP.4
ADO_IGS.1	AGD_ADM.1	
ADV_FSP.2	ADV_RCR.1	
ADV_HLD.2	ADV_FSP.1 ADV_RCR.1	covered by ADV_FSP.2
ADV_IMP.2	ADV_LLD.1 ADV_RCR.1 ALC_TAT.1	
ADV_LLD.1	ADV_HLD.2 ADV_RCR.1	
ADV_RCR.1	–	
ADV_SPM.1	ADV_FSP.1	covered by ADV_FSP.2
AGD_ADM.1	ADV_FSP.1	covered by ADV_FSP.2
AGD_USR.1	ADV_FSP.1	covered by ADV_FSP.2
ALC_DVS.1	(no dependencies)	
ALC_LCD.1	(no dependencies)	

Security Assurance Requirements		
Component	Dependency	Remark
ALC_TAT.1	ADV_IMP.1	covered by ADV_IMP.2
ATE_COV.2	ADV_FSP.1 ATE_FUN.1	covered by ADV_FSP.2
ATE_DPT.1	ADV_HLD.1 ATE_FUN.1	covered by ADV_HLD.2
ATE_FUN.1	(no dependencies)	
ATE_IND.2	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	covered by ADV_FSP.2
AVA_CCA.1	ADV_FSP.2 ADV_IMP.2 AGD_ADM.1 AGD_USR.1	
AVA_MSU.2	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	
AVA_SOF.1	ADV_FSP.1 ADV_HLD.1	covered by ADV_FSP.2 covered by ADV_HLD.2
AVA_VLA.4	ADV_FSP.1 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1 AGD_ADM.1 AGD_USR.1	covered by ADV_FSP.2 covered by ADV_IMP.2

Table 6-5 Justification of Unsupported Dependencies

TOE-Security Functional Requirements		
Component	Dependency	Justification
FAU_GEN.1	FPT_STM.1	FAU_GEN.1 uses sequence data, which may be a sequence number or reliable time stamp. If sequence number is used FPT_STM.1 is not needed. The application not directs the ST editor to include FPT_STM.1 if reliable time stamp is used by the TOE.
FCS_COP.1/ SCD_Export	[FDP_ITC.1 or FCS_CKM.1], FMT_MSA.2	The PP does not requires a specific form of the key management for Subcsriber-SCD transfer because different solution are possible. The application note advices the ST writer to solve the dependencies.
FDP_IFC.1	FDP_IFF.1	The component FDP_IFF.1 is addressed by the component FDP_IFF.4

Table 6-6 IT-Environment Security Functional Requirements Dependencies

Security Functional Requirements for the IT Environment		
Component	Dependency	Remark
FAU_SAR.1/ENV	FAU_GEN.1	not fulfilled (see below)
FAU_STG.1/ENV	FAU_GEN.1	not fulfilled (see below)
FCS_COP.1/SCD_Import	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	not fulfilled (see below)
FTP_ITC.1/SCD_Import	(no dependencies)	
FTP_ITC.1/SVD_Import	(no dependencies)	
FTP_TRP.1/CLIENT	(no dependencies)	

Application Note:
The dependencies for the IT-Environmental Security Functional Requirements are not solved to allow a wide range of possible solutions. Therefore it is left to the editor of the ST to fulfil these dependencies or to justify their non-fulfilment to meet the objectives they are grounding in.

6.4 Security Functional Requirements Grounding in Objectives

The mapping of the TOE Security Functional Requirements grounding in Objectives are given in 6.2.1 in table 2.

Table 6-5 Security Assurance Requirements to Objective mapping.

Requirement	Security Objectives
Security Assurance Requirements	
ACM_AUT.1	EAL4
ACM_CAP.4	EAL4
ACM_SCP.2	EAL4
ADO_DEL.2	EAL4
ADO_IGS.1	EAL4
ADV_FSP.2	EAL4
ADV_HLD.2	EAL4
ADV_IMP.2	augmented (ADV_IMP.2 required by AVA_CCA.1)
ADV_LLD.1	EAL4
ADV_RCR.1	EAL4
ADV_SPM.1	EAL4
AGD_ADM.1	EAL4

Requirement	Security Objectives
AGD_USR.1	EAL4
ALC_DVS.1	EAL4
ALC_LCD.1	EAL4
ALC_TAT.1	EAL4
ATE_COV.2	EAL4
ATE_DPT.1	EAL4
ATE_FUN.1	EAL4
ATE_IND.2	EAL4
AVA_CCA.1	augmented (not required by EAL4)
AVA_MSU.2	EAL4
AVA_SOF.1	EAL4
AVA_VLA.4	augmented (AVA_VLA.2 required by EAL4)

6.5 Rationale for Extensions

This PP defines extension to CC part 2 [3] for quality of random numbers used to generate Subscriber-SCD. No extensions to CC part 3 [4] have been incorporated in this PP.

6.5.1 Rationale for Extension of Class FCS with Family FCS_RND

The TOE shall generate Subscriber-SCD with high cryptographic quality using random number generators. The family FCS_RNG.1 requires the ST editor to define the quality metric of the random numbers used by the TOE to generate the Subscriber-SCD. The component FCS_RND.1 similar to FCS_RND.1 in CC part 2 is limited in their application to secrets used as authentication information.

FCS_RND generation of random numbers

Family behaviour

This family defines quality metrics for generating random numbers intended for cryptographic purposes.

Component levelling

FCS_RND.1 The generation of random numbers using TSFs requires the random numbers to meet the defined quality metrics.

Management: FCS_RND.1

No management functions are provided for.

Audit: FCS_RND.1

There are no events identified that should be auditable if FCS_RND generation of random numbers data generation is included in the PP/ST.

FCS_RND.1 Quality metrics for random numbers

Hierarchical to: no other components.

FCS_RND.1.1 The TSFs shall provide a mechanism for generating random numbers that meet [assignment: *a defined quality metric*].

FCS_RND.1.2 The TSFs shall be able to enforce the use of TSF-generated random numbers for [assignment: *list of TSF functions*].

Dependencies: FPT_TST.1 TSF testing.

6.6   Rationale for Assurance Level 4 Augmented

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

      ADV_IMP.2   Development - Implementation of the TSF
      AVA_CCA.1   Vulnerability Assessment - Covert channel analysis
      AVA_VLA.4   Vulnerability Assessment - Vulnerability Analysis – Highly resistant

The security objective O.Subs-SCD_Secure includes protection against disclosing completely or partly the Subscriber-SCD through any physical or logical TOE interface. This calls for security functional requirements as FDP_IFF.4/Crypto and security assurance requirements as AVA_CCA.1. ADV_IMP.2 is required to fulfil the dependencies for AVA_CCA.1.

The TOE generates, uses and manages the most sensitive data of the signatory – the Subscriber-SCD. The TOE shall be shown to be highly resistant to penetration attacks. Any loss of confidentiality or integrity of the Subscriber-SCD threaten the security of the all signatures generated with this Subscriber-SCD. The cryptographic security of the Subscriber-SCD/CSP-SVD pair generation can be ensured only by the TOE itself. The TOE shall be free of any covert channel which might compromise the Subscriber-SCD. The TOE environment shall support the TOE in Subscriber-SCD protection against physical and some other attacks but cannot make up for TOE security. The protection of the Subscriber-SCD shall be solely and in tabloid form provided by the CM as part of the trustworthy system. The complex protection of the Subscriber-SCD requires a systematic and complete vulnerability analysis by SAR AVA_VLA.4. Therefore the strength of function "high" for AVA_SOF.1 and AVA_VLA.4 Highly resistant is chosen.

Appendix A - References

[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 2.1, August 1999

[3]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements; Version 2.1, August 1999

[4]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 2.1, August 1999

[5]	ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures V1.1.1 (2003-03).

[6]	European Telecommunications Standards Institute Technical Specification, *ETSI TS 101462 Policy requirements for certification authorities issuing qualified certificates,* V1.1.1, 2000.

[7]	European Committee for Standardization CEN/ISSS: *Security Requirements of Secure Signature Creation Devices (SSCD) – SSCD-PP,* CWA 14169:2002 E.

[8]	Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999

Appendix B - Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SAR	Security assurance requirements
SFP	Security Function Policy
SFR	Security functional requirements
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy