

CEN

CWA 14167-3

WORKSHOP

June 2003

AGREEMENT

ICS 03.120.20; 35.040

English version

**Security Requirements for Trustworthy Systems Managing
Certificates for Electronic Signatures - Part 3: 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, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Luxembourg, Malta, Netherlands, Norway, Portugal, Slovakia, 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

© 2003 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. CWA 14167-3:2003 D/E/F

Table of Contents

Foreword	5
Conventions and Terminology	7
Conventions	7
Terminology	7
Document Organisation	9
1 Introduction	10
1.1 Identification	10
1.2 Protection Profile Overview	10
2 TOE Description	12
2.1 TOE Roles	12
2.2 TOE Usage	12
3 TOE Security Environment	14
3.1 Assets to protect	14
3.2 Assumptions	14
3.3 Threats to Security	15
3.4 Organisational Security Policies	17
4 Security Objectives	17
4.1 Security Objectives for the TOE	17
4.2 Security Objectives for the Environment	18
5 IT Security Requirements	20
5.1 TOE Security Functional Requirements	20
5.1.1 Security audit (FAU)	20
5.1.2 Cryptographic support (FCS)	22
5.1.3 User data protection (FDP)	22
5.1.4 Identification and authentication (FIA)	25
5.1.5 Security management (FMT)	26
5.1.6 Protection of the TOE Security Functions (FPT)	28
5.2 TOE Security Assurance Requirements	31
5.2.1 Configuration management (ACM)	32
5.2.2 Delivery and operation (ADO)	33
5.2.3 Development (ADV)	34
5.2.4 Guidance documents (AGD)	36
5.2.5 Life cycle support (ALC)	37
5.2.6 Tests (ATE)	38
5.2.7 Vulnerability assessment (AVA)	39
5.3 Security Requirements for the IT Environment	41
5.3.1 Security audit (FAU)	41
5.3.2 User data protection (FDP)	41
5.3.3 Trusted path/channels (FTP)	41
5.3.4 Non-IT requirements	42
6 Rationale	43
6.1 Introduction	43
6.2 Security Objectives Rationale	44
6.2.1 Security Objectives Coverage	44
6.2.2 Security Objectives Sufficiency	45
6.3 Security Requirements Rationale	50
6.3.1 Security Requirement Coverage	50

6.3.2	Security Requirements Sufficiency	52
6.4	Dependency Rationale	55
6.4.1	Functional and Assurance Requirements Dependencies	55
6.5	Security Functional Requirements Grounding in Objectives	59
6.6	Rationale for Extensions	60
6.7	Rationale for Assurance Level 4 Augmented	60
References		61
Appendix A - Acronyms		61

List of Tables

Table 5.1 Assurance Requirements: EAL 4 augmented	31
Table 6-1 Security Environment to Security Objective Mapping	44
Table 6-2 Functional and Assurance Requirement to Security Objective Mapping	50
Table 6-3 TOE Security Functional Requirements Dependencies	55
Table 6-4 Security Assurance Requirements Dependencies	57
Table 6-5 IT-Environment Security Functional Requirements Dependencies	58
Table 6-6 Justification of Unsupported Dependencies	58
Table 6-7 Security Assurance Requirements to Objective mapping.	59

Foreword

The production of this CEN Workshop Agreement (CWA) This 'Cryptographic Module for CSP Key Generation Services - Protection Profile' (CMCKG-PP) was agreed by the CEN/ISSS Electronic Signatures Workshop (WS/E-SIGN) in its meeting in Naples on 24 April 2002, in the context of the European Electronic Signature Standardization Initiative (EESSI).

This CWA has been developed through the collaboration of a number of contributing partners in the E-SIGN Workshop, gathering a wide mix of interests, representing different sectors of industry (manufacturers, end-users, service providers, legal experts, academia, accreditation bodies, standardization organisations and national standards bodies) as well as representatives of the national public and European authorities.

The present CWA has received the support of representatives of these sectors. A list of company experts who have supported the document's contents may be obtained from the CEN/ISSS Secretariat.

The final review/endorsement round for this CWA was started on 2002-10-07 and was successfully closed on 2002-11-04. The final text of the PPs was submitted to CEN for publication on 2003-04-03.

The CWA 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.

The CWA has been prepared as a Protection Profile (PP) following the rules and formats of ISO 15408, as known as the Common Criteria version 2.1 [2] [3] [4].

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:

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

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

Email iss@cenorm.be

— 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). This Protection Profile (PP) represents Annex A to the CWA that has been developed by the European Electronic Signature Standardisation Initiative (EESSI) CEN/ISSS electronic signature (E-SIGN) workshop, Area D2 on trustworthy systems.

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-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.

CWA 14167-3:2003 (E)

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)

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 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, Helmut Kurth, Herbert Leitold, Hans Nilsson
Vetting Status:	
CC Version:	2.1 Final
General Status:	WS/E-Sign draft for public comments
Version Number:	0.07 draft
Registration:	
Keywords:	cryptographic module, CSP, key generation

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)).

and

- a) CA-generated subscriber keys shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures.*

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.

- 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 Signature Creation Data (SCD).

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 conformant 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 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:

- Signature Creation Data (SCD): private key of subscribers, created internally in the TOE and loaded into an SSCD Type 2
- Signature Verification Data (SVD): public key of subscriber, created internally in the TOE and transferred into an SSCD Type 2, 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 read audit data generated by the TOE and exported for audit review in the TOE environment. 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 SCD against disclosure, compromise and unauthorized modification and for ensuring that the TOE services are only used in an authorized way.

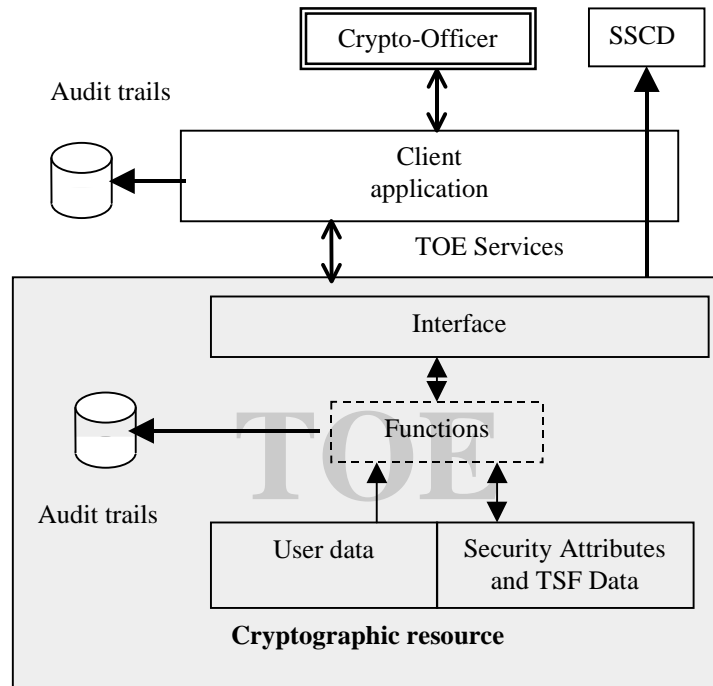


Figure 1: TOE general overview

The TOE is used to generate 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 SCD / SVD pairs for the integration into the SSCD of subscribers. The confidentiality of the SCD as well as the integrity and authenticity of both the SCD and the 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 SCD during transfer and the requirements to protect a single 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 internal data:

- **Subscriber-SCD:** Signature-creation data generated for the subscriber of the certification service provider. The subscriber-SCD shall be protected in confidentiality and integrity.
- **Subscriber-SVD:** Signature-verification data generated for the subscriber of the certification service provider. The subscriber-SVD shall be protected in integrity.
- **R.DATASUBS:** 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.HARDWARE:** hardware parts of the TOE have to be protected in integrity and availability.
- **R.SOFTWARE:** software parts of the TOE have to be protected in integrity.
- **R.SERVICES:** integrity of the TOE services as well as protection against misuse is required.

3.2 Assumptions

A.Audit_Support *CSP audit review*

The CSP reviews the audit trail generated and exported by the TOE.

A.Human_Interface *Interface with Human Users*

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

A.User_Management *User Management*

The management of the individual users for the Crypto-user roles except the client application is performed in the TOE environment. It is assumed that this is done in a secure way according to a well defined policy.

3.3 Threats to Security

T.Bad_Init *Initialisation of the TOE that does not Result in a Secure State*

Before the TOE can be used it has to be initialised correctly to get into a secure state to start normal operation. Any failure in this initialisation process may result in a state that does not provide the required quality of the keys generated or the required protection of user key material.

T.Bad_SW_Load *Loading Malicious Software during the Lifetime of the TOE*

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

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 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.Malfunction *Malfunction of TOE*

Internal malfunction of TOE functions may result in the generation of subscriber-SCD of low quality or invalid 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. 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.Management *Exploitable Initialisation, management and start-up*

Assets are revealed in TOE initialisation, start-up and operation due to attack during initialisation and by management.

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

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

CWA 14167-3:2003 (E)

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 secret keys or to misuse services of the TOE.

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 Type 2 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.SSCD_Misuse *Misuse of SSCD before and after transfer of the SCD*

Subscriber-SSCD may be misused before the SCD is transferred and after this transfer has been performed. A particular threat is the use of SSCD by persons other than their legitimate owner. Note: The legitimate owner of a SSCD may change in the different life-cycle stages of a SSCD.

T.Defect *Physical Defects of the TOE*

The TOE may contain physically defects which prevents it to perform its services. This includes the destruction of the TOE as well as hardware failures which prevent the TOE from performing its services. This includes also the destruction of the TOE by deliberate action or environmental failure.

T.Insecure_Init *Insecure Initialisation of the TOE*

The TOE may be initialised in an insecure environment, by unauthorised personnel or without using adequate organisational controls.

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.Theft *Stealing the TOE*

The theft of all or part of the TOE may result in a loss of confidentiality (direct effect), integrity (authentication device) and/or availability.

T.Data_Manipul *Manipulating Data outside of the TOE*

Data that is transmitted to the TOE from the client application may be manipulated within the TOE environment before it is passed to the TOE. This may result in the effect that the TOE signs data without the approval of the user under whose control the command to generate a SCD/SVD pair is submitted to the TOE. When performed within the client application such manipulations may not be detectable by the TOE itself and therefore this threat needs to be countered within the *TOE* environment.

Manipulation of data in the TOE environment within the session of a Crypto-officer may also result in a compromise of the security of the TOE. If the TOE supports backup of user data and TSF data these data might be lost.

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 SCD/SVD pair generation for secure electronic signatures. This includes the generation of random numbers, the post-processing of random numbers, the random number test procedures and the tests on the quality of the SCD/SVD pairs generated (e. g. primality tests). Where confidentiality protection is required such as for the transfer of SCD to the user devices, only algorithms and algorithm parameters defined as acceptable for that purpose 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
- Initializing the trusted channel to the remote trusted IT product (in case of an on-line transfer)
- Unsuccessful authentication
- Modification of TOE management data
- Adding new users or roles
- Deleting users or roles
- Unsuccessful self test operations
- Reading and deleting audit trail records

The integrity of the audit trail shall be ensured. The TOE shall export the audit data upon request of user within a role allowed to access the audit data.

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.

CWA 14167-3:2003 (E)

O.Check_Operation *Check for Correct Operation*

The TOE shall perform regular checks to verify that its components operate correctly.

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 error. 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 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 SVD exported to CGA or to the SSCD Type2.

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_Application *Security in the Client Application*

The applications which use the TOE shall perform the necessary security checks on the data passed to the TOE. The applications shall also perform the required user authentication and access control functions that can not be performed within the TOE. Security controls in the TOE environment shall also prevent unauthorised manipulation of data submitted to 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.

O.ENV_Protect_Access *Prevention of Unauthorised Physical Access*

The TOE shall 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_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 SCD to SSCD*

The SSCD Type2 shall ensure the confidentiality of the SCD transferred from the TOE. In case the SVD is also transferred from the TOE to the SSCD Type2, it shall ensure its integrity.

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

The CGA or the SSCD Type2 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 not specified level of audit; and
- c)
 - (1) Initialisation of the TOE,
 - (2) Start-up after power-up,
 - (3) Shutdown of the TOE,
 - (4) Software download if supported by the TOE,
 - (5) Cryptographic key generation (FCS_CKM.1): subscriber-SCD/CSP-SVD pair generation,
 - (6) Cryptographic key destruction (FCS_CKM.4): destruction of keys used to establish the trusted channel (FCS_CKM.4),
 - (7) Export of user data without security attributes (FDP_ETC.1): number of keys exported,
 - (8) Authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts and the actions,
 - (9) Timing of authentication (FIA_UAU.1): all unsuccessful use of the authentication mechanism,
 - (10) Management of security attributes (FMT_MSA.1)/(all instantiations): all modifications of the values of security attributes,
 - (11) Static attribute initialisation (FMT_MSA.3/CRYPTO_AUDIT): modifications of the default setting of permissive or

- restrictive rules, all modifications of the initial values of security attributes;
- (12) Management of TSF data (FMT_MTD.1/ACCESS CONTROL): All modifications to the values of TSF data.
 - (13) Management of TSF data (FMT_MTD.1/AUDIT: Export of audit data, Clear of audit data.
 - (14) Abstract machine testing (FPT_AMT.1): Execution of the tests of the underlying machine and the results of the tests.
 - (15) Failure with preservation of secure state (FPT_FLS.1): Failure detection of the TSF and secure state.
 - (16) Notification of physical attack (FPT_PHP.2): Detection of intrusion.
 - (17) TSF testing (FPT_TST.1): Execution of the TSF self tests and the results of the tests.
 - (18) 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.

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 metric for saving audit records defined by the CSP 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

CWA 14167-3:2003 (E)

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: List of approved algorithms and parameters.

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 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.

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 Crypto-SFP on User; Subscriber-SCD, Subscriber-SVD; generate Subscriber-SCD/SVD pair (FCS_CKM.1), destruction of Subscriber-SCD and Subscriber-SVD (FCS_CKM.4).

5.1.3.2 Subset access control (FDP_ACC.1/AUDIT)

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

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

FDP_ACF.1.1/
CRYPTO The TSF shall enforce the Crypto-SFP to objects based on Identity and Role.

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) User with security attribute Role Crypto-Officer is allowed to generate (FCS CKM.1) the objects Subscriber-SCD and Subscriber-SVD
- (2) User with security attribute Role Crypto-Officer is allowed to export (FDP UCT.1, FTP ITC.1) the object Subscriber-SCD.
- (3) User with security attribute Role Crypto-Officer is allowed to export (FTP ITC.1) the object Subscriber-SVD

FDP_ACF.1.3/
CRYPTO The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/
CRYPTO The TSF shall explicitly deny access of subjects to objects based on the following rules: User with security attribute Auditor is not allowed to

- (a) generate (FCS CKM.1) the objects Subscriber-SCD and Subscriber-SVD,
- (b) export (FDP UCT.1, FTP ITC.1) the objects Subscriber-SCD and Subscriber-SVD.

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

FDP_ACF.1.1/
AUDIT The TSF shall enforce the Audit-SFP to objects based on Identity and Role.

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: Users with the role attribute Auditor are allowed

- (1) to export Audit data,
- (2) to clear Audit data.

FDP_ACF.1.3/
AUDIT The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none.

FDP_ACF.1.4/
AUDIT The TSF shall explicitly deny access of subjects to objects based on the rule: Users with security attribute Role Crypto-officer are not allowed to delete Audit data

Application note:

Users with the role Crypto-officer may be allowed to read audit data without export or deleting it.

5.1.3.5 Subset information flow control (FDP_IFC.1/CRYPTO)

FDP_IFC.1.1/
CRYPTO The TSF shall enforce the 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).

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

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

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

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 de-allocation of the resource from the following objects: subscriber-SCD.

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 integrity errors on all objects, based on the following attributes: error detecting code.

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

Application Note:

The integrity of the subscriber-SCD may be checked with the subscriber SVD as error detecting code by verifying the created signature by signature verification.

5.1.3.9 Basic data exchange confidentiality (FDP_UCT.1)

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

Application Note:

This applies 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 block the identity for authentication.

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: identity and role.

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 TSF Generation of secrets (FIA_SOS.2)

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet a defined quality metric according to the list of approved algorithms and parameters.

FIA_SOS.2.1 The TSF shall be able to enforce the use of TSF generated secrets for FCS_CKM.1.

5.1.4.5 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow 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) 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.

5.1.4.6 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow 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) 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 determine the behaviour of the function audit (FAU_GEN.1) to Auditor.

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

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

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

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

FMT_MSA.1.1/
USER_CRYPTO The TSF shall enforce the Crypto-SFP to restrict the ability to delete the security attributes Identity and RAD for user with role attribute Crypto-officer to Crypto-officer.

FMT_MSA.1.1/
USER_AUDIT The TSF shall enforce the Audit-SFP to restrict the ability to delete the security attributes Identity and RAD for user with role attribute Auditor to the role assigned to perform the export and evaluation of audit records.

5.1.5.4 Management of security attributes (FMT_MSA.1/RAD)

FMT_MSA.1.1/
RAD The TSF shall enforce the Crypto-SFP and Audit-SFP to restrict the ability to modify the security attributes RAD to User for its own RAD.

5.1.5.5 Secure security attributes (FMT_MSA.2)

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

5.1.5.6 Static attribute initialisation (FMT_MSA.3/CRYPTO_AUDIT)

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

FMT_MSA.3.2/
CRYPTO_AUDIT The TSF shall allow the Auditor to specify alternative initial values to override the default values when an object or information is created.

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

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

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

FMT_MTD.1.1/
AUDIT The TSF shall restrict the ability to query the audit data of the TSF required by FAU_GEN.1 to [assignment: *the authorised identified roles*].

Application note:

The Auditor is allowed to query, export and delete the audit data. The Crypto-officer may be allowed to read audit data without export or deleting it.

5.1.5.9 Specification of Management Functions (FMT_SMF.1)

- FMT_SMF.1.1** The TSF shall be capable of performing the following security management functions:
1. Definition of the audit function behaviour (FMT_MOF.1.1/AUDIT)
 2. Management of the notification of the local user about detected physical attacks (FPT_PHP.2)
 3. User management (FMT_MSA.1/ROLE, FMT_MSA.1/USER, FMT_MSA.1/RAD)
 4. Management of audit data (FMT_MOF.1.1/AUDIT, FMT_MSA.3.2/CRYPTO_AUDIT, FMT_MTD.1/AUDIT).

5.1.5.10 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles Crypto-Officer and Auditor.

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

Application note:

A specific TOE may have defined additional roles. This is allowed as long as the definition of those roles is compliant with the requirements stated in this PP. Especially none of these 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 at the request of an authorised user 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: failures detected by the TSF FPT_AMT.1 and FPT_TST.1.

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 local user 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.

5.1.6.4 Resistance to physical attack (FPT_PHP.3)

- FPT_PHP.3.1 The TSF shall resist physical tampering by opening the device or removal of a cover to the components which
- generates Subscriber-SCD (FCS CKM.1)
- stores Subscriber-SCD
- stores other secret or private keys
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 during initial start-up, at the request of the authorised user, at the conditions and at installation and maintenance 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 generated signature before the signature is exported). Supplementary tests shall detect error of the random number generator used for the generation of Subscriber-SCD (see FCS_CKM.1 and FIA_SOS.2), 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 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 The TSF shall permit the TOE to initiate communication via the trusted channel.

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

Application Note:

The TOE shall provide a trusted channel between itself and either the subscriber SSCD or another trusted IT product that securely transfers the SCD to the subscriber SSCD. This trusted channel needs to protect the integrity and the confidentiality of the Subscriber-SCD. In addition there is the requirement to transfer the Subscriber SVD to the CGA via a trusted channel that protects the integrity of the SVD or to the subscriber SSCD or to both.

The trusted channel should be established by means of cryptographic mechanisms.

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.
- 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 CM documentation.

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.

ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

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

ADO_IGS.1.1D The developer shall document procedures necessary for the 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

CWA 14167-3:2003 (E)

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.1.1C 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.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.
- 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.1.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

ALC_LCD.1.1D The developer shall establish a life-cycle model to be used in the

CWA 14167-3:2003 (E)

development and maintenance of the TOE.

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

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

5.2.5.3 Well-defined development tools (ALC_TAT.1)

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

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

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

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

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

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.1.1C 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.

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

5.2.6.3 Functional testing (ATE_FUN.1)

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

ATE_FUN.1.1D The developer shall test the TSF and document the 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.1.2D The developer shall provide test documentation.
- 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.1.1C The analysis documentation shall identify covert channels and estimate their capacity.
- AVA_CCA.1.1D The developer shall conduct a search for covert channels for each information flow control policy.
- 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.1.2D The developer shall provide covert channel analysis documentation.
- 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 and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.
- AVA_VLA.4.2D The developer shall document the disposition of identified vulnerabilities.
- AVA_VLA.4.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.
- AVA_VLA.4.2C The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.

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

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

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 The TSF shall provide System auditor of the CSP with the capability to read all audit information produced by the TOE from the audit records.
/ENV

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

5.3.1.2 Protected audit trail storage (FAU_STG.1)

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

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records.
/ENV

5.3.2 User data protection (FDP)

5.3.2.1 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1 The TSF shall enforce the [assignment: access control SFP(s) and/or information flow control SFP(s)] to be able to [selection: transmit, receive] user data in a manner protected from [selection: modification, deletion, insertion, replay] errors.
/ENV

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [selection: modification, deletion, insertion, replay] has occurred.
/ENV

5.3.3 Trusted path/channels (FTP)

5.3.3.1 Trusted path (FTP_TRP.1)

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

FTP_TRP.1.2 The TSF shall permit local users to initiate communication via the trusted path.
/CLIENT

CWA 14167-3:2003 (E)

FTP_TRP.1.3 /CLIENT The TSF shall require the use of the trusted path for communication with TOE for identification, authentication and management.

5.3.3.2 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 /SSCD 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 /SSCD The TSF shall permit [selection: the TSF, the remote trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 /SSCD The TSF shall initiate communication via the trusted channel for SCD import.

FTP_ITC.1.1 /SVD import 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 import The TSF shall permit [selection: the TSF, the remote trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 /SVD import The TSF shall initiate communication via the trusted channel for SVD import.

Application notes

The SVD may be imported by the certification-generation application or by the SSCD for storing and future export to a certification-generation application. The trusted channels should be established by means of cryptographic mechanisms.

5.3.4 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 Introduction

The TOE that has been defined covers cryptographic modules that implement—partly or completely—the functionality necessary for devices involved in generating the Subscriber-SCD and Subscriber-SVD. The tables in sub-sections 6.2.1 “Security Objectives Coverage” and 6.3.1 “Security Requirement Coverage” provide the mapping of the security objectives and security requirements for these TOE types.

6.2 Security Objectives Rationale

6.2.1 Security Objectives Coverage

Table 6-1 Security Environment to Security Objective Mapping

	T.Bad_init	T.Bad_SW_Load	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.Defect	T.Insecure_Init	T.Insecure_Oper	T.Theft	T.Data_Manipul	T.SSCD_Misuse	A.Audit_Support	A.Human_interface	A.User_Management	P.Algorithms
O.Audit_CM	x	x			x	x	x													
O.Subs_SCD_Secure			x	x																x
O.Check_Operation					x						x									
O.Control_Services	x	x				x	x													
O.Detect_Attack								x												
O.Error_secure					x			x			x									
O.SCD_Transfer				x					x											
O.SVD_Transfer										x										
O.User_authentication		x				x														
O.ENV_Application												x			x			x		
O.ENV_Audit																	x			
O.ENV_Human_interface																		x		
O.ENV_Personnel		x										x	x			x	x		x	
O.ENV_Protect_Access													x	x						
O.ENV_Secure_Init												x				x				
O.ENV_Secure_Oper			x	x							x		x						x	
O.ENV_SCD_Transfer				x					x						x					
O.ENV_SVD_Transfer										x										

6.2.2 Security Objectives Sufficiency

6.2.2.1 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 SCD/SVD pair generation within the key generation process. This includes the generation of random numbers, the post-processing of random numbers, the random number test procedures and the tests on the quality of the SCD/SVD pairs generated (e. g. primality tests). Where confidentiality protection is required such as for the transfer of 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) ensures the confidentiality and integrity of the subscriber-SCD 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.

6.2.2.2 Threats and Security Objective Sufficiency

T.Bad_init (Initialisation of the TOE that does not Result in a Secure State) deals with the threat that any failure in this initialisation process may result in a state that does not provide the required protection of the SCD and the TOE services. This results from the necessity that before the TOE can be used it has to be initialised correctly to get into a secure state to start normal operation. **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.

T.Bad_SW_Load (Loading 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 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 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 threat that the most valuable asset the TOE has to protect are the Subscriber-SCD 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 SCD using knowledge about the key generation process. **O.Subs-SCD_Secure** (Secure Subscriber-SCD Generation and Management) ensures the confidentiality and integrity of the Subscriber-SCD as long as they are under the control of the TOE. The TOE shall ensure cryptographic secure subscriber-SCD/SVD pair generation and

CWA 14167-3:2003 (E)

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 as addressed by **O.Subscriber-SCD_Derive** or over any physical or logical TOE interface as addressed by **O.Subscriber-SCD_Disclosure**. 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. Furthermore this security objective requires that the SCD shall be deleted from the TOE whenever it is exported from that TOE to prevent disclosure after use by the TOE. **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 SCD, misuse of TOE services, disclosure or distortion 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. **O.Audit_CM** (Audit record generation and export) shall audit unsuccessful self test operations. **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.

T.Management (Exploitable Initialisation, management and startup) addresses the threat that assets are revealed in TOE initialisation, start-up and operation due to attack during initialisation and by management. **O.Audit_CM** (Audit record generation and export) ensures the audit of TOE initialisation, TOE startup, 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.

T.Misuse (Misuse of SCD/SVD pair generation function) addresses the threat that an attacker misuses the TOE for generation of SCD/SVD pairs. This may result in SCD/SVD pairs that are used without proper authorization. The **O.Audit_CM** (Audit record generation and export) shall audit the generation and destruction of Subscriber-SCD. **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.

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.

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 SCD. **O.SCD_Transfer** (Secure transfer of Subscriber-SCD to the SSCD) and the **O.ENV_SCD_Transfer** (Secure import of SCD to SSCD) provides that the SCD is transmitted via secure channel to the SSCD Type 2 ensuring the confidentiality of the SCD. Moreover the SCD shall be deleted by the TOE 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 Type 2 if it stores the SVD for later transmission to the CGA. The **O.SVD_Transfer** and the **O.ENV_SVD_Transfer** requires the TOE and the IT environment (CGA or SSCD) together to ensure the integrity of the SVD.

T.Defect (Physical Defects of the TOE) deals with the threat that the TOE may contain physically defects which prevents it to perform its services. This includes the destruction of the TOE as well as hardware failures which prevent the TOE from performing its services. This includes also the destruction of the TOE by deliberate action or environmental failure. **O.Check_Operation** (Check for Correct Operation) ensures regular checks to verify that its components operate correctly performed by the TOE. **O.Error_secure** (Secure state in case of error) forces 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. **O.ENV_Secure_Oper** (Secure Operating Procedures) provides procedures and controls defined 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.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.ENV_Application** (Security in the Client Application) ensures that the applications shall also perform the required user authentication and access control functions that can not be performed within the TOE. Security controls in the TOE environment shall also prevent unauthorised manipulation of data submitted to the TOE. **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

CWA 14167-3:2003 (E)

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. **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.

T.Theft (Stealing the TOE) describes the threat that the theft of all or part of the TOE in a loss of confidentiality (direct effect), integrity (authentication device) and/or availability. **O.ENV_Protect_Access** (Prevention of Unauthorised Physical Access) ensures that the TOE shall 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.

T.Data_Manipul (Manipulating Data outside of the TOE) describes the threat that data which are transmitted to the TOE from the client application may be manipulated within the TOE environment before they are passed to the TOE. This may result in the effect that the TOE signs data without the approval of the user under whose control the command to generate a SCD/SVD pair is submitted to the TOE. When performed within the client application such manipulations may not be detectable by the TOE itself and therefore this threat needs to be countered within the TOE environment. Manipulation of data in the TOE environment within the session of a Crypto-officer may also result in a compromise of the security of the TOE. If the TOE supports backup of user data and TSF data these data might be lost. **O.ENV_Application** (Security in the Client Application) provides that the applications which use the TOE shall perform the necessary security checks on the data passed to the TOE. The applications shall also perform the required user authentication and access control functions that can not be performed within the TOE. Security controls in the TOE environment shall also prevent unauthorised manipulation of data submitted to the TOE. **O.ENV_SCD_Transfer** (Secure import of SCD to the SSCD) provides that the SSCD Type2 ensures the confidentiality of the SCD transferred from the TOE. In case the SVD is also transferred from the TOE to the SSCD Type2, it shall ensure its integrity.

T.SSCD_Misuse (Misuse of SSCD before and after transfer of the SCD) deals with the threat that the Subscriber SSCD may be misused before the SCD is transferred and after this transfer has been performed. A particular threat is the use of SSCD by persons other than their legitimate owner. Note: The legitimate owner of a SSCD may change in the different life-cycle stages of a SSCD. **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. **O.ENV_Secure_Init** (Secure Initialisation Procedures) deals with the definition and application of procedures and controls in the TOE environment that allow to securely set-up and initialise the TOE for the generation Subscriber-SCD/SVD pairs. This includes the initial configuration of other TSF data like roles, users and user authentication information.

6.2.2.3 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 if the TOE does not have a human interface for authentication and management services the client application will provide an appropriate interface and communication path between human users and the TOE. The TOE environment transmits identification, authentication and management data of TOE users correctly and in a confidential way to the TOE. This is fulfilled by the following two objectives: **O.ENV_Application** (Security in the Client Application) provides that the applications shall perform the required user authentication and access control functions that can not be performed within the TOE. Security controls in the TOE environment shall also prevent unauthorised manipulation of data submitted to the TOE. **O.ENV_Human_Interface** (Reliable Human Interface) ensures in case 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.

A.User_Management (User Management) the management of the individual users for the Crypto-user roles except the client application is performed in the TOE environment. It is assumed that this is done in a secure way according to a well defined policy. **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. **O.ENV_Secure_Oper** (Secure Operating Procedures) provides the definition of 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.

6.3 Security Requirements Rationale

6.3.1 Security Requirement Coverage

Table 6-2 Functional and Assurance 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_Application	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																
FDP_ACC.1/CRYPTO				x														
FDP_ACC.1/AUDIT	x			x														
FDP_ACF.1/CRYPTO				x														
FDP_ACF.1/AUDIT	x			x														
FDP_IFC.1/CRYPTO		x																
FDP_IFF.4/CRYPTO		x																
FDP_RIP.1		x																
FDP_SDI.2		x																
FDP_UCT.1							x											
FIA_AFL.1									x									
FIA_ATD.1									x									
FIA_SOS.1									x									
FIA_SOS.2																		
FIA_UAU.1									x									
FIA_UID.1									x									
FMT_MOF.1/AUDIT	x																	
FMT_MOF.1/PHYS					x													
FMT_MSA.1/ROLE				x					x									
FMT_MSA.1/ USER_CRYPTO				x					x									
FMT_MSA.1/ USER_AUDIT				x					x									
FMT_MSA.1/RAD				x					x									
FMT_MSA.2				x														
FMT_MSA.3/CRYPTO				x														
FMT_MTD.1/ACCESS				x														
FMT_MTD.1/AUDIT	x			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_Application	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
FMT_SMF.1	x			x	x				x									
FMT_SMR.1				x														
FPT_AMT.1			x			x												
FPT_FLS.1						x												
FPT_PHP.2					x													
FPT_PHP.3					x													
FPT_RCV.1						x												
FPT_TST.1			x	x		x												
FTP_ITC.1							x	x										
ACM_CAP.4				x														
ADO_DEL.2				x														
ADO_IGS.1				x														
ALC_DVS.1				x														
ALC_LCD.1				x														
AVA_CCA.1		x																
AVA_VLA.4		x																
FAU_SAR.1/ENV											x							
FAU_STG.1/ENV											x							
FCS_COP.1/ENV																		
FDP_UIT.1/ENV										x								
FTP_TRP.1/CLIENT												x						
FTP_ITC.1/SSCD																	x	x
FTP_ITC.1/CGA																		x
RE.ENV_Personnel													x					
RE.ENV_Protect_Acce														x				
RE.ENV_Secure_Init															x			
RE.ENV_Secure_Oper																x		

The security assurance components not indicated in the table are required by the EAL 4 package and its augmentations.

6.3.2 Security Requirements Sufficiency

6.3.2.1 TOE Security Requirements Sufficiency0

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 under control of the SFR **FDP_ACC.1/AUDIT** (Subset access control), **FDP_ACF.1/AUDIT** (Security attribute based access control), **FMT_MTD.1/AUDIT** (Management of TSF data), **FMT_MOF.1/AUDIT** (Management of security functions behaviour) and **FMT_SMF.1** (Specification of Management Functions) specify the requirements of the management of the audit function. The behaviour of the audit function is managed by the Auditor role separated from Crypto-officer role by **FMT_MSA.1** (all instantiations). The integrity of the audit data will be ensured by the SFR **FAU_STG.2/TOE** (Guarantees of audit data availability) inside the TOE

O.Subs-SCD_Secure (Secure Subscriber-SCD Generation and Management) addresses the security of the Subscriber-SCD.

The cryptographic security of the SCD is implemented by the SFR **FCS_CKM.1** (Cryptographic key generation). 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 **FDP_IFC.1/CRYPTO** (Subset information flow control) and **FDP_IFF.4/CRYPTO** (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, Crypto-officer and Crypto-user as defined by the SFR **FMT_SMR.1** (Security roles). The SFR **FMT_MOF.1/AUDIT** (Management of security functions behaviour), **FMT_MOF.1/PHYS** (Management of security functions behaviour), **FMT_MSA.1/ROLE** (Management of security attributes), **FMT_MSA.1/USER_Crypto** (Management of security attributes), **FMT_MSA.2** (Secure security attributes), **FMT_MSA.3/CRYPTO_AUDIT** (Static attribute initialisation), **FMT_MTD.1/ACCESS_CONTROL** (Management of TSF data), **FMT_MTD.1/AUDIT** (Management of TSF data) and **FMT_SMF.1** (Specification of Management Functions) assign

the management functions for the cryptographic and audit functions to the Auditor or Crypto-officer. The SFR **FMT_MSA.1/USER_CRYPTO** (Management of security attributes) and **FMT_MSA.1/RAD** (Management of security attributes) provide to restrict the ability to modify the default values and to delete the security attributes which may be changed by the Crypto-officer and the RAD-Owner. The SFR **FMT_MSA.1/USER_AUDIT** (Management of security attributes) and **FMT_MSA.1/RAD** (Management of security attributes) provide to restrict the ability to modify the default values and to delete the security attributes which may be changed by the Auditor and the RAD-Owner. Note that the user management is addressed by O.User_authentication. The SFR **FPT_TST.1** 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.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 is managed according to **FMT_MOF.1/PHYS** (Management of security functions behaviour) and **FMT_SMF.1** (Specification of Management Functions). The refinements limit 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.

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 (Protection of TSF Data Exported by the TOE) 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).

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 SSCD Type2. This protection is provided by means of a trusted channel by the TOE by **FTP_ITC.1** (Inter-TSF trusted channel) and supported by the CGA of the SSCD Type 2 by **FTP_ITC.1/SVD import**.

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 identified respectively 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 SFR **FIA_AFL.1** (Authentication failure handling) protects the RAD against guessing. The SFR for the Management of security attributes **FMT_MSA.1/ROLE**, **FMT_MSA.1/USER_CRYPTO**, **FMT_MSA.1/USER_AUDIT**, **FMT_MSA.1/RAD** and **FMT_SMF.1** (Specification of Management Functions) separate the roles Auditor and Crypto-officer.

6.3.2.2 TOE Environment Security Requirements Sufficiency

O.ENV_Application (Security in the Client Application) addresses the client application which acts as agent for the end-user gaining access to the TOE key generation, transfer functions and audit functions. The client application may implement the human interface and for the end-user identification and authentication required by the TOE SFR **FIA_UID.1** (Timing of identification) and **FIA_UAU.1** (Timing of authentication). If the client application provides this human interface it shall protect this communication by a trusted path **FPT_TRP.1/CLIENT**. Security controls in the TOE environment shall also prevent unauthorised manipulation of data submitted to the TOE as required by SFR **FDP_UIT.1/ENV** (Data exchange integrity).

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 **FPT_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 SCD to SSCD) shall ensure the confidentiality and the integrity of the SCD transferred from the TOE to the SSCD Type2. Both functions are provided by the SFR **FTP_ITC.1/SSCD** (Inter-TSF trusted channel).

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 SSCD Type2 or both. In those cases the CGA or the SSCD shall provide the trusted channel provided by the SFR **FTP_ITC.1/SVD import** and supported by the TOE by **FPT_ITC.1**.

6.4 Dependency Rationale

6.4.1 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	
FAU_STG.2/TOE	FAU_GEN.1	
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4 FMT_MSA.2	The TOE generates, exports and delete the Subscriber-SCD but does not use them for signing. Therefore FCS_COP.1 for the Subscriber-SCD is not included.
FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1 FMT_MSA.2	FCS_CKM.1 is included.
FDP_ACC.1/CRYPTO	FDP_ACF.1/CRYPTO	
FDP_ACC.1/AUDIT	FDP_ACF.1/AUDIT	
FDP_ACF.1/CRYPTO	FDP_ACC.1/CRYPTO FMT_MSA.3/CRYPTO_AU DIT	
FDP_ACF.1/AUDIT	FDP_ACC.1/AUDIT FMT_MSA.3/CRYPTO_AU DIT	

CWA 14167-3:2003 (E)

Security Functional Requirements		
Component	Dependency	Remark
FDP_IFC.1/CRYPTO	FDP_IFF.1	not fulfilled, information flow policy is implemented by FDP_IFF.4
FDP_IFF.4/CRYPTO	AVA_CCA.1 FDP_IFC.1/CRYPTO	
FDP_RIP.1	–	
FDP_SDI.2	–	
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1 FDP_ACC.1 or FDP_IFC.1	FTP_ITC.1
FIA_AFL.1	FIA_UAU.1	
FIA_ATD.1	–	
FIA_SOS.1	–	
FIA_SOS.2	–	
FIA_UAU.1	FIA_UID.1	
FIA_UID.1	–	
FMT_MOF.1.1/AUDIT	FMT_SMF.1, FMT_SMR.1	
FMT_MOF.1.1/PHYS	FMT_SMF.1, FMT_SMR.1	
FMT_MSA.1/ROLE	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1, FMT_SMR.1	FDP_ACC.1 and FDP_IFC.1
FMT_MSA.1/USER_Crypto	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1, FMT_SMR.1	FDP_ACC.1 and FDP_IFC.1
FMT_MSA.1/USER_AUDIT	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1, FMT_SMR.1	FDP_ACC.1 and FDP_IFC.1
FMT_MSA.1/RAD	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1, FMT_SMR.1	FDP_ACC.1 and FDP_IFC.1
FMT_MSA.2	ADV_SPM.1 FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	FDP_ACC.1 and FDP_IFC.1
FMT_MSA.3/CRYPTO_AUDIT	FMT_MSA.1 FMT_SMR.1	
FMT_MTD.1/ACCESS_CONTROL	FMT_SMF.1, FMT_SMR.1	
FMT_MTD.1/AUDIT	FMT_SMF.1, FMT_SMR.1	
FMT_SMF.1	–	
FMT_SMR.1	FIA_UID.1	
FPT_AMT.1	–	
FPT_FLS.1	ADV_SPM.1	
FPT_PHP.2	FMT_MOF.1/PHYS	
FPT_PHP.3	–	
FPT_RCV.1	FPT_TST.1 AGD_ADM.1 ADV_SPM.1	
FPT_TST.1	FPT_AMT.1	
FTP_ITC.1	–	

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	–	
ALC_LCD.1	–	
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	–	
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 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)
FDP_UIT.1/ENV	FDP_ACC.1 or FDP_IFC.1 FTP_ITC.1 or FTP_TRP.1	not fulfilled (see below) both fulfilled
FIA_UAU.1/ENV	FIA_UID.1	
FIA_UID.1/ENV	–	
FTP_TRP.1/ENV	–	
FTP_ITC.1/ENV	–	

Application Note:

The dependencies for the IT-Environmental Security Functional Requirements (ESFR) are not yet solved. 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.

Table 6-6 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.
FDP_IFC.1/CRYPTO	FDP_IFF.1	The component FDP_IFF.1 is addressed by the component FDP_IFF.4
FPT_PHP.2	FMT_MOF.1	FPT_PHP.2 informs the local user about detected tampering attempts. No management functions behaviour is needed.

6.5 Security Functional Requirements Grounding in Objectives

The mapping of the TOE Security Functional Requirements grounding in Objectives are given in 6.3.1 in table 2.

Table 6-7 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
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)

6.6 Rationale for Extensions

No extensions to CC part 2 [3] or CC part 3 [4] have been incorporated in this PP.

6.7 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.

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] Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the 'Electronic Signature Committee' in the Directive.
- [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.

Appendix A - 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
TSFI	TSF Interface
TSP	TOE Security Policy