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

WORKSHOP AGREEMENT

CWA 14167-2

March 2002

ICS 03.120.20; 35.040

Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)

Ref. No CWA 14167-2:2002 E

Rue de Stassart, 36 • B-1050 Bruxelles
Tel : +32 2 550 08 11 • Fax : +32 2 550 08 19

—— this page has intentionally been left blank ——

Foreword

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

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

This CEN Workshop Agreement 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 2001-09-11 and was successfully closed on 2001-12-07. The final text of this CWA was submitted to CEN for publication on 2002-01-11.

The CWA14167 on "Security Requirments for Trustworthy Systems Managing Certificates for Electronic Signatures" is currently composed of two parts:
Part 1: System Security Requirements
Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)

The CEN/ISSS Electronic Signatures Workshop may develop further parts to this as part of its ongoing work programme

The document 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 Signing Operations - Protection Profile (CMCSO-PP) should be referred to:

CONTACT ADDRESS

CEN/ISSS Secretariat
Rue de Stassart 36
1050 Brussels, Belgium
Tel *+32 2 550 0813*
Fax *+32 2 550 0966*
Email *isss@cenorm.be*

—— this page has intentionally been left blank ——

—— this page has intentionally been left blank ——

Table of Contents

—— this page has intentionally been left blank ——

List of Tables

—— this page has intentionally been left blank ——

Conventions and Terminology

Conventions

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

Terminology

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

Advanced electronic signature (defined in the Directive [1], article 2.2) means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control, and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

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

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

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

CSP signature creation data (CSP-SCD) means SCD which is used by the CSP, e.g. for the creation of advanced electronic signatures in qualified certificates or for signing certificate status information.

CSP signature verification data (CSP-SVD) means SVD which corresponds to the CSP-SCD and which is used to verify the advanced electronic signature in the qualified certificate.

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).

Data to be signed (DTBS) means the complete electronic data to be signed, such as QC content data or certificate status information.

Data to be signed representation (DTBS-representation) means the data sent to the TOE for signing and is

(a) a hash-value of the DTBS or
(b) an intermediate hash-value of a first part of the DTBS and a remaining part of the DTBS or
(c) the DTBS itself.

The client indicates to the TOE the case of DTBS-representation, unless implicitly indicated. The hash-value in case (a) or the intermediate hash-value in case (b) is calculated by the client. The final hash-value in case (b) or the hash-value in case (c) is calculated by the TOE.

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 advanced signature in qualified certificates and which represents the TOE.

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

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

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).

Side-channel means illicit information flow in result of the physical behavior 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 behavior 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.

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 Signing Operations – Protection Profile
Authors:	Wolfgang Killmann, Helmut Kurth, Herbert Leitold, Hans Nilsson
Vetting Status:	
CC Version:	2.1 Final
General Status:	approved by CEN/ISSS WS-ESIGN on 2001-12-07
Version Number:	0.18 approved
Registration:	
Keywords:	cryptographic module, CSP signing device, qualified certificate signing, certificate status information signing

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 CA keys are generated in accordance with industry standards, and*
- *The CA shall ensure that CA private keys remain confidential and maintain their integrity".*

[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.**

This Protection Profile (PP) defines the security requirements of a Cryptographic Module (CM) used by CSP as part of its trustworthy system to provide signing services, such as Certificate Generation Service or Certificate Status Information Signing Services. The Cryptographic Module, which is the Target of Evaluation (TOE), is used for the creation of CSP private keys, and their usage for the creation of advanced electronic signatures in qualified certificates or certificate status information. Such keys are referred to in this PP as Certificate Signature Creation Data (CSP-SCD).

The TOE may implement additional functions and security requirements, e.g. for the creation of Signature Creation Data (SCD) for loading into Secure Signature Creation Devices (SSCD) as part of a Subscriber Device Provision Service. However, these additional functions and security requirements are not subject of this Protection Profile.

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), in accordance with this procedure.

2 TOE Description

The TOE is a Cryptographic Module (CM) used for the creation and usage of Certificate Signature Creation Data (CSP-SCD). The CM may optionally also perform hashing of the qualified certificate content.

The TOE is configured software and hardware that may be used to provide the following cryptographic functions:

- Generation of Certificate Signature Creation Data (CSP-SCD)
- Usage of the CSP-SCD to create advanced electronic signatures for qualified certificates based on either
  a) the hash value of the content of the qualified certificate, or
  b) the complete content of the qualified certificate, where the hashing is also performed in the CM (optional).

The Protection Profile's primary scope is for signing qualified certificates. Still components evaluated against this standard may be applied for other signature-creation tasks carried out by a certificate service provider (CSP) such as time-stamping, signing certificate revocation lists (CRLs) or issuing online certificate status protocol (OCSP) messages.

For the cryptographic functions, the TOE shall support the cryptographic algorithms specified in [5], or a subset thereof.

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

- User authentication
- Access control for the creation and destruction of keys
- Access control for usage of keys to create certificate signatures
- Auditing of security-relevant changes to the TOE
- Self-test of the TOE

The TOE shall handle the following User Data:

- CSP Signature Creation Data (CSP-SCD): private key of CSP, created and stored internally in the TOE, with optional provision of key backup and restore functions
- Data to be signed representation (DTBS-representation): The data to be signed by the TOE may e.g. be:
  - Certificate hash value: imported to the TOE
  - Certificate contents (optional, when hashing is performed in the TOE), data to be hashed and signed, imported to the TOE
  - other data to be signed by the TOE, such as CRL or the hash value of the CRL, or time-stamping content data
  - Certificate signature: created signature, exported from the TOE.

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 and to create, destruct, backup/restore CSP-SCDs)
- Crypto-user (authorized to sign with existing CSP-SCDs)
- Auditor (authorized to read audit data generated by the TOE and exported for audit review in the TOE environment)

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.

The interface to the TOE may either be shared between the different user categories, or separated for certain functions, for example configuration and key backup/restore. 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 CSP-SCD against disclosure, compromise and unauthorized modification and for ensuring that the TOE services are only used in an authorized way.

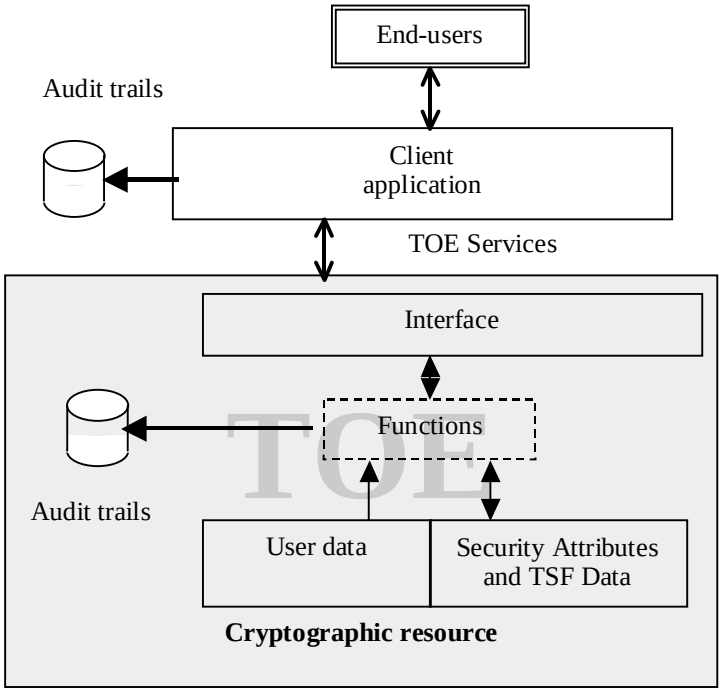


Figure 1: TOE general overview

As shown in figure 1, end-users will communicate with the client application, which in turn will call TOE services on behalf of the end-user. The client application is responsible for passing any user data in a correct way to the TOE. Different mechanisms may be used to protect the user data on its way from the originating user to the TOE, but all those mechanisms are not part of the TOE functionality and therefore not defined in this Protection Profile.

It is the responsibility of the client application in the TOE environment to identify and authenticate the end-users, and map their identity to a role in the TOE (Crypto-user), based on access control rules in the TOE environment. It is the responsibility of the TOE environment to perform identity-based auditing to support accountability for the cryptographic operations. While the TOE will only perform auditing for the client application the TOE environment audit might distinguish between the end-users of the client application.

The client application that communicates with the TOE may itself consist of different parts implemented on different systems. For example, a client application that initiates the generation of qualified certificate may consist of two parts:

1. A registration application, which initialises the information for the certificate.

2. A signature-creation application which may be

    a) a certification application, which verifies the integrity and authenticity of the request submitted by the registration application and then calls the TOE service to sign the certificate or

b) other applications requesting the TOE to sign DTBS-representations, e.g. certificate status information. The application verifies integrity and authenticity of the signature request.

In this case, the registration application may perform user based authentication for the registration officer to ensure that the certification request has been generated by an authorised registration facility while the certification application and the TOE perform an identity based authentication for the client application only.

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:

- **R.DATAUSER**: confidential user data (CSP-SCD, other user related secret keys (if any), user / role authentication data, etc.). Those data has to be protected both in confidentiality and integrity.
- **R.USERMGMT**: non-confidential user / role related data (identifier, access control lists, role definitions, etc.). Those data has to be protected in integrity.
- **R.DATASYSTEM**: other system data not related to a user or role (system configuration data, audit data)
- **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.

Data shared between the TOE and its environment:

- **R.BACKUP**: backup data exported by the TOE to be backed up in the TOE environment. This data needs to be protected in integrity and confidentiality (if required) by the TOE. Availability of this data has to be ensured in the TOE environment.
- **R.DATAEXCH**: data exchanged by the TOE through its interface (parameters for services that can be activated through the interface). They have to be protected in integrity. Some of those imported data shall also be protected in confidentiality (encipher keys, verification authentication data).

Services ensured by the TOE:

- **R.SERVICES**: integrity and availability 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.Correct_DTBS *Correct DTBS Content Data*

DTBS-representation submitted to the TOE is assumed to be correct. This requires that the DTBS (e.g. the certificate content data) has been initialised correctly and maintains this correctness until it is passed to the TOE. This requires the DTBS to be correctly defined during the registration process, be transferred with integrity protection between the systems involved in the process (e.g. registration and certificate generation), be processed in a correct way by the client application, being hashed correctly (in the case the hashing is done by the client application and not by the TOE) and passed correctly to the TOE.

The TOE environment will probably use its own mechanisms to ensure this correctness during processing and transmission. This will for example include mechanisms that can be used to verify the integrity and authenticity of user data when passed between different entities within the TOE environment. Specific instantiations of the TOE may have additional functions that can be used by the TOE environment to maintain the integrity of user data outside of the TOE, but those functions are not mandated by this Protection Profile

A.Data_Store *Storage and Handling of TOE data*

Critical TOE data may be stored outside of the TOE. Examples are backup data for software, CSP-SCD, other cryptographic keys, and TOE configuration data. Although the TOE is required to ensure the necessary confidentiality and integrity protection of this data, the environment has to ensure the availability of this data.

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_Authentication *Authentication of Users*

The client-application is assumed as user of the TOE in the Crypto-user role. Other users authorised for the TOE Crypto-user services may be not be known to the TOE itself. The TOE environment performs identification and authentication for theses individual users and allows successfully authenticated users to use the client application as their agent for the Crypto-user services.

Application note:

There are different users of the TOE services within a CSP environment. The TOE itself is only required to relate a request for a TOE service to a specific role and requires credentials to authenticate that the request was generated by a user having a specific role. In the following section we discuss the TOE role model and the users within the TOE environment.

In most cases the registration authority is separated from the certificate generation system. The registration authority system usually has its own protection features including the identification and authentication of individual users (“registration officers”) of the specific registration authority system.

Once the certificate request has been generated on the registration authority system it is submitted to the certificate generation system protected by a digital signature. This digital

signature is used by the certificate generation system to verify that the request has been issued by a registration authority authorised to generate certification requests for this certificate generation system.

The registration authority may use its own internal user management and the individual users within the registration authorities may not be known to the certificate generation system and therefore also not known to the TOE. The registration authority may use one specific RA private key to sign a certification request and may use its own internal audit procedures to relate a specific certification request to an individual user within the RA system.

Maintenance of the TOE as well as the management of the CSP-SCDs is highly critical operations that need to be related to the individual users that performed the operation. It is therefore required that for the roles System Administrator and Crypto Administrator of the CSP [7] the individual users for those roles have to be known by the TOE as Crypto-officer and the TOE needs to perform user based authentication for those roles. The Crypto-officer role is very powerful including user and key management. Therefore the Auditor role is implemented to watch on Crypto-officer's actions and to detect misuse of Crypto-officer's authorization.

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.

Application Note

Management of the individual users for the System Administrator and the Crypto Administrator role needs to be performed within the TOE as Crypto-officer.

3.3 Threats to Security

3.3.1 Threats to be countered by the TOE

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 protection of the CSP-SCD and the TOE services.

If the TOE supports backup of CSP-SCD, other user data and TSF data an attacker may manipulate the backup data to initialise the TOE insecurely by the restore procedure.

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.CSP-SCD_Derive *Deriving All or Parts of the CSP-SCD*

The most valuable asset the TOE has to protect is the CSP-SCD. The ability to derive all or parts of the CSP-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 CSP-SCD using knowledge about the CSP-SCD generation process.

T.CSP-SCD_Disclose *Disclosing All or Part of the CSP-SCD*

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

T.CSP-SCD_Distortion *Distortion of the CSP-SCD*

When the CSP-SCD is distorted, DTBS signed with the distorted CSP-SCD (e.g. qualified certificates or CRLs) will be invalid. Although the use of a distorted CSP-SCD can be detected, the impacts for the organisation issuing the signed data using the CSP-SCD (e.g. qualified certificates) can be high. There is also the danger that by the use of a distorted CSP-SCD, parts of the original CSP-SCD can be derived.

T.Malfunction *Malfunction of TOE*

Internal malfunction of TOE functions may result in the modification of DTBS-representation, misuse of TOE services, disclosure or distortion of CSP-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 the CSP-SCD, the modification of DTBS-representation 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
- storage devices used to store the CSP-SCD or the DTBS-representation
- 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 signature-creation function*

An attacker misuses the TOE for signature-creation. This may result in forged signed data, such as forged qualified certificates or forged certificate status information.

T.Phys_Manipul *Physical Manipulation of the TOE*

An attacker may try to physically manipulate the TOE with the intent to derive all or part of the CSP-SCD, to manipulate the DTBS within the TOE or to misuse services of the TOE.

T.Signature_Forgery *Forgery of digital signature*

An attacker exploits weaknesses in the cryptography and/or key management in the TOE in order to forge a CSP digital signature in a way that is not detectable by the verifier of the signature.

3.3.2 Threats to be countered by the TOE environment

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 data 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 (e. g. key length) defined as acceptable for being used for signature-creation by trustworthy systems shall be used to e.g. generate qualified certificates or to sign certificate status information. Where confidentiality protection is required such as for

backup of CSP-SCD, 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 CSP-SCD
- Destruction of CSP-SCD
- 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.Backup *Backup and Restore for the TOE*

If the TOE supports backup of CSP-SCD, other user data and TSF data to restore an operational state after failure the TOE will protect the confidentiality of the backup data and detect loss of the integrity of the backup data.

Application note:
The backup support of the TOE is optional. Therefore all TOE security requirements specific for the security objective O.Backup are collected in the Backup package.

O.CSP-SCD_Secure *Secure CSP-SCD Generation and Management*

The confidentiality and integrity of the CSP-SCD shall be ensured during their whole life time. The TOE shall ensure cryptographic secure CSP-SCD generation, use and management. This includes protection against disclosing completely or partly the CSP-SCD through any physical or logical TOE interface.

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 the CSP-SCD in this case.

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 the CSP-SCD.

O.Protect_Exported_Data *Protection of TSF Data Exported by the TOE*

The TOE shall apply integrity and confidentiality protection measures to all assets listed in the asset list requiring integrity or confidentiality protection when they are exported from the TOE e.g. for the purpose of backup.

O.Sign_Secure *Secure advanced signature-creation*

The TOE creates signatures such as the advanced signature in qualified certificates that

- do not reveal the CSP-SCD and
- can not be forged without knowledge of the CSP-SCD.

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_Backup *Secure Handling of Backup Media*

Data transmitted by the TOE to be backed up in the TOE environment shall be stored in a way which ensures the availability of the backup data in the case a restore is required.

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_Recovery *Secure Recovery in Case of Major Failure*

Recovery plans and procedures shall exist that allow a secure and timely recovery in the case of a major problem with the TOE. These procedures shall ensure that the confidentiality and integrity of TOE assets are maintained during recovery and that the recovery does not result in a situation that allows personnel to extend the TOE services they are allowed to use.

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 of signatures for qualified certificates or certificate status information. This includes the secure key generation / key import as well as 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.

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

Basic Package

5.1.1 Security audit (FAU)

5.1.1.1 Audit data generation (FAU_GEN.1/BASIC)

FAU_GEN.1.1/ BASIC — 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) Initialisation of the TOE,
Start-up after powerup,
Shutdown of the TOE,
Cryptographic key generation (FCS_CKM.1): CSP-SCD/CSP-SVD pair generation,
Cryptographic key destruction (FCS_CKM.4): CSP-SCD destruction, backup key(s) destruction Backup package,
Authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts and the actions,
Timing of authentication (FIA_UAU.1): all unsuccessful use of the authentication mechanism,
Management of security attributes (FMT_MSA.1) /(all instantiations): all modifications of the values of security attributes,
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;
Management of TSF data (FMT_MTD.1/ACCESS_CONTROL): All modifications to the values of TSF data,
Management of TSF data (FMT_MTD.1/AUDIT: Export of audit data, Clear of audit data,
Abstract machine testing (FPT_AMT.1): Execution of the tests of the underlying machine and the results of the tests,
Failure with preservation of secure state (FPT_FLS.1): Failure detection of the TSF and secure state,
Notification of physical attack (FPT_PHP.2): Detection of intrusion,
TSF testing (FPT_TST.1): Execution of the TSF self tests and the results of the tests.

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, identity of the user and sequence data

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

Application note:
The audit data for the Crypto-user role can only identify the client application. Further refinement of audit data might be provided by audit functions in the TOE environment distinguishing between end-users using the services of the client application.
If time stamps are chosen as the sequence data the ST shall include security functional requirements for reliable time stamps (FPT_STM.1).

5.1.1.2 User identity association (FAU_GEN.2/BASIC)

FAU_GEN.2.1/ BASIC 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 overwritten the audit trail data after reading (export) by the Crypto-officer. The ST shall perform the assignment for the metric for saving audit records according the storage provided for audit events. This metric should implement security mechanisms to ensure availability of audit data in case of audit storage exhaustion because of limited storage of audit events. For example, if the storage is exhausted, the TOE would

(i) stop the normal operation,
(ii) inform the actual user about exhaustion of the audit event storage and
(iii) continue the normal operation only after export and deletion of audit data.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*assignment: cryptographic key generation algorithm*] and specified cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: 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 the CSP-SCD and all other plaintext secret or private keys, if the TSF required by FPT_PHP.2 detects physical tampering.

5.1.2.3 Cryptographic operation (FCS_COP.1/Sign)

FCS_COP.1.1/SIGN The TSF shall perform digital signature-creation in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: List of approved algorithms and parameters.

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; CSP-SCD, CSP-SVD, DTBS representation; generate CSP-SCD/CSP-SVD pair (FCS_CKM.1), destruction of CSP-SCD and CSP-SVD (FCS_CKM.4); DTBS representation (FCS_COP.1/SIGN).

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)

Crypto-SFP

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 CSP-SCD and CSP-SVD under dual person control.
(2) User with security attribute Role Crypto-officer is allowed to destruct (FCS_CKM.4) the objects CSP-SCD and CSP-SVD.
(3) User with security attribute Role Crypto-user is allowed to create signature of the DTBS-representation with CSP-SCD (FCS_COP.1/SIGN).

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 roles: User with security attribute Role Crypto-user is not allowed

(a) generate (FCS_CKM.1) the objects CSP-SCD and CSP-SVD,
(b) destruct (FCS_CKM.4) the objects CSP-SCD and CSP-SVD.

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

Audit-SFP

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 security attribute Role 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 following roles

1. Users with security attribute Role Crypto-officer are not allowed to export or to delete Audit data
2. Users with security attribute Role Crypto-user are not allowed to export or to delete Audit data.

5.1.3.5 Export of user data without security attributes (FDP_ETC.1)

FDP_ETC.1.1 — The TSF shall enforce the Crypto-SFP when exporting user data, controlled under the SFP(s), outside of the TSC.

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

5.1.3.6 Extended user private and secret key export (FDP_ETC_KEY.1)

FDP_ETC_KEY.1.1 — CSP-SCD shall only be exported from the TOE in encrypted form.

FDP_ETC_KEY.1.2 — Secret keys and private keys other than CSP-SCD shall be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret or private keys shall be exported from the TOE in encrypted form.

5.1.3.7 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 CSP-SCD; generation of CSP-SCD/SVD pair (FCS_CKM.1), destruction of CSP-SCD (FCS_CKM.4), signing DTBS-representation (FCS_COP.1/SIGN).

5.1.3.8 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
(1) the CSP-SCD/SVD generation (FCS_CKM.1),
(2) the signature-creation (FCS_COP.1/SIGN),
through physical behaviour of the TOE interfaces and emanation [assignment: other relevant side-channels] compromising information about the CSP-SCD to a maximum capacity.

FDP_IFF.4.2/ CRYPTO — The TSF shall prevent the following types of side-channels within the data exported
(1) by the TSF CSP-SCD / SVD pair generation (FCS-CKM.1),
(2) by the TSF signature-creation function (FCS-COP.1/SIGN) about the CSP-SCD.

Application note:
The TSF requires the TOE to prevent side-channel attacks against the CSP-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 CSP-SCD through the intended output data of the TOE e.g. the random padding bits in the signature generated by the same unsuitable pseudo-random number generator as the CSP-SCD itself.

5.1.3.9 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: CSP-SCD and VAD.

5.1.3.10 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.

Refined by adding:
The TSF are not required to monitor the DTBS representation for integrity errors.

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

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 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.

5.1.5.2 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 change_default and delete the security attributes Identity and VAD for user with role attribute Crypto-officer and Crypto-user to Crypto-officer.

FMT_MSA.1.1/ USER_AUDIT The TSF shall enforce the Audit-SFP to restrict the ability to change default and delete the security attributes Identity and VAD for user with role attribute Auditor to Auditor.

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

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

5.1.5.4 Secure security attributes (FMT_MSA.2)

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

5.1.5.5 Static attribute initialisation (FMT_MSA.3/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.

5.1.5.6 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.

5.1.5.7 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/BASIC to Crypto-officer.

5.1.5.8 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles Crypto-officer and Crypto-user.

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

Application note:
The Crypto-user role may be associated with only one user – the client application. The client application in the TOE environment may act as agent for more than one user demanding singing of DTBS by the HSM.

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 SCP-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 For TOE, 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.

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 CSP-SCD (FCS_CKM.1)
- creates the signature with CSP-SCD (FCS_COP.1)
- stores CSP-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 SCP-SCD and other confidential secret and private keys if physical tampering performed by opening the device or removal of a cover is detected.

Application Note:

The TOE shall protect the confidentiality of the SCP-CSD and other secret and private keys in case of physical maintenance or physical tampering. 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 CSP-SCD in case of loss of power. The TSF will invoke the TSF required by FCS_CKM.4 to destroy the SCP-SCD and all other plaintext secret and private keys. The destruction of the CSP-SCD will prevent the use of an attacked TOE for signing 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, 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/SIGN). 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 CSP-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.

Backup Package

The backup support of the TOE is optional. Therefore all TOE security requirements specific for the security objective O.Backup are collected in this Backup package.

5.1.7 Security audit (FAU)

5.1.7.1 Audit data generation (FAU_GEN.1/Backup)

FAU_GEN.1.1/ BACKUP — 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) Cryptographic key distribution (FCS_CKM.2/BACKUP): entry of back-up key(s)
Cryptographic key destruction (FCS_CKM.4): destruction of backup key(s)
Backup and recovery (FDP_BKP.1): Use of the backup function, Use of the recovery function, Unsuccessful recovery because of detection of modification of the backup data
Inter-TSF detection of modification (FPT_ITI.1): The detection of modification of imported backuped TSF data

FAU_GEN.1.2/ BACKUP — 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:
The sequence data shall be a sequence number of the audit event data or time stamp.

Application Note:

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

5.1.7.2 User identity association (FAU_GEN.2/Backup)

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

5.1.8 Cryptographic support (FCS)

5.1.8.1 Cryptographic key distribution (FCS_CKM.2/BACKUP)

FCS_CKM.2.1/ BACKUP — The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method key entry that meets the following: [*assignment: list of standards*].

Refinement
The key entry shall be performed using either manual or electronic methods. All encrypted secret or private keys entered into the TOE shall be encrypted using a cryptographic algorithm from the list of approved algorithms and parameters. [5]
Secret and private keys established using manual methods shall be entered either

(1) in encrypted form or
(2) using split knowledge procedures.

If split knowledge procedures are used:

(1) The TOE shall separately authenticate the crypto-officer entering each key component.
(2) At least two key components shall be required to reconstruct the original cryptographic key.

Manually-entered keys shall be verified during entry into the TOE for accuracy.
Secret and private keys established using electronic methods shall be entered in encrypted form.

Application note:
The TSF shall import the backup key(s) at least to restore the TOE to an operational status at a previous point in time.

5.1.8.2 Cryptographic operation (FCS_COP.1/BACKUP_ENC)

FCS_COP.1.1/ BACKUP_ENC — The TSF shall perform encryption and decryption in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: list of approved algorithms and parameters.

Application note:
The TSF shall use a backup key

5.1.8.3 Cryptographic operation (FCS_COP.1/BACKUP_INT)

FCS_COP.1.1/ BACKUP_INT — The TSF shall perform calculation and verification of cryptographic checksums in accordance with a specified cryptographic algorithm [*assignment: cryptographic algorithm*] and cryptographic key sizes [*assignment: cryptographic key sizes*] that meet the following: list of approved algorithms and parameters.

Application note:
The cryptographic checksum shall use a backup key and shall be based on symmetric cryptographic algorithms (e.g. keyed hash) or asymmetric cryptographic algorithms (e.g. digital signatures).

5.1.9 User data protection (FDP)

5.1.9.1 Subset access control (FDP_ACC.1/BACKUP)

FDP_ACC.1.1/ BACKUP — The TSF shall enforce the Backup SFP on User; CSP-SCD, backup key(s), backup data; backup (FDP_BKP.1), restore (FDP_BKP.1), backup key entry (FCS_CKM.2/BACKUP).

5.1.9.2 Security attribute based access control (FDP_ACF.1/BACKUP)

Backup-SFP

FDP_ACF.1.1/ BACKUP — The TSF shall enforce the Backup SFP to objects based on Identity and Role.

FDP_ACF.1.2/ BACKUP — The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: User with security attribute Role Crypto-officer is allowed under dual person control

(a) to backup CSP-SCD and CSP-SVD (FDP_BKP.1),
(b) to restore CSP-SCD and CSP-SVD (FDP_BKP.1),
(c) to enter backup keys (FCS_CKM.2/BACKUP)

FDP_ACF.1.3/ BACKUP — The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: rules, based on security attributes that explicitly authorise access of subjects to objects.

FDP_ACF.1.4/ BACKUP — The TSF shall explicitly deny access of subjects to objects based on the User with security attribute Role Crypto-user is not allowed

(a) to backup CSP-SCD,
(b) to restore CSP-SCD,
(c) to enter a backup key (FCS_CKM.2/BACKUP).

Application note:

If the TSF implementing FDP_BKP.1 does not support separate backup for CSP-SCD and for other backup data the additional rules in FDP_ACF.1.3 may allow the Crypto-officer to backup and to restore all backup data.

5.1.9.3 Backup and recovery (FDP_BKP.1)

FDP_BKP.1.1 The TSF shall include a backup function.

FDP_BKP.1.2 The Crypto-officer shall be capable of invoking the backup function on demand.

FDP_BKP.1.3 The data stored in the backup shall be sufficient to recreate the state of the TOE at the time the backup was created using only:

(1) a copy of the same version of the TOE as was used to create the backup data;
(2) a stored copy of the backup data;
(3) the cryptographic key(s) needed to decrypt the CSP-SCD and any other encrypted critical security parameters;
(4) the cryptographic key(s) needed to verify the cryptographic checksum of the backup data.

FDP_BKP.1.4 The TSF shall include a recovery function that is able to restore the state of the TOE from a backup.

FDP_BKP.1.5 The CSP-SCD, other critical security parameters and other confidential information shall be stored in encrypted form only.

FDP_BKP.1.6 The backup data shall be checked for modification through the use of cryptographic checksums. Modified backup data shall not be used for recovery.

5.1.9.4 Subset information flow control (FDP_IFC.1/BACKUP)

FDP_IFC.1.1/ BACKUP The TSF shall enforce the Side-channel of backup-functions SFP on Anybody; Information about CSP-SCD; backup (FDP_BKP.1, FCS_COP.1/BACKUP_ENC, FCS_COP.1/BACKUP_INT), restore (FDP_BKP.1, FCS_COP.1/BACKUP_ENC, FCS_COP.1/BACKUP_INT), key entry (FCS_CKM.2/BACKUP).

5.1.9.5 Partial elimination of illicit information flows (FDP_IFF.4/BACKUP)

FDP_IFF.4.1/ BACKUP — The TSF shall enforce the Side-channel of backup-functions SFP to limit the capacity of covert channels of

(1) the backup function including encryption of the backup data (FDP_BKP.1),
(2) the backup key(s) entry (FCS_CKM.2),
(3) the encryption and decryption of the backup data (FCS_COP.1/BACKUP_ENC)

through physical behaviour of the TOE interfaces and emanation [assigment: other relevant side-channels] compromising information about the CSP-SCD to a maximum capacity.

FDP_IFF.4.2/ BACKUP — The TSF shall prevent the following types of side-channels within the backup data (FDP_BKP.1) about the CSP-SCD.

Application note:
The TOE shall prevent side-channel attacks against the CSP-SCD and other secret data where the attack is based on external observable physical phenomena of the TOE as mentioned in the application note to FDP_IFF.4/Crypto. The maximum capacity of the side channels shall be defined by the ST allowing the SCP to prevent any remaining side channels by appropriate security measures in the TOE environment.
The TOE shall prevent side-channel attacks against the CSP-SCD through the intended output data of the TOE e.g. the backup data encrypted with an initial vector containing information about the used backup key.

5.1.10 Security management (FMT)

The security functional requirements FMT_MSA.1/BACKUP_ROLE, FMT_MSA.1/BACKUP_USER, FMT_MSA.1/BACKUP_VAD and FMT_MSA.3/BACKUP extend FMT_MSA.1/ROLE, FMT_MSA.1/USER FMT_MSA.1/VAD and FMT_MSA.3/CRYPTO_AUDIT to enforce the backup SFP if the TOE supports backup.

5.1.10.1 Management of security attributes (FMT_MSA.1/BACKUP_ROLE)

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

5.1.10.2 Management of security attributes (FMT_MSA.1/BACKUP_USER)

FMT_MSA.1.1/ BACKUP_USER — The TSF shall enforce the Backup SFP to restrict the ability to change default and delete the security attributes Identity and VAD to Crypto-officer.

5.1.10.3 Management of security attributes (FMT_MSA.1/BACKUP_VAD)

FMT_MSA.1.1/ BACKUP_VAD: The TSF shall enforce the Backup SFP to restrict the ability to modify the security attributes VAD to User for its own VAD.

5.1.10.4 Static attribute initialisation (FMT_MSA.3/BACKUP)

FMT_MSA.3.1/ BACKUP: The TSF shall enforce the Backup SFP to provide restrictive default values for security attributes that are used to enforce the SFP.

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

5.1.10.5 Inter-TSF confidentiality during transmission (FPT_ITC.1)

FPT_ITC.1.1	The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorised disclosure during transmission.

Application note:
The SFR FPT_ITC.1 addresses the confidentiality protection of the TSF data if they are exported as part of the backup data.

5.1.10.6 Inter-TSF detection of modification (FPT_ITI.1)

FPT_ITI.1.1	The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: cryptographic checksum according to the list of approved algorithms and parameters.
FPT_ITI.1.2	The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform alarm indication to the Crypto-officer if modifications are detected.

Application note:
The SFR FPT_ITI.1 addresses the integrity protection of the TSF data if they are imported as part of the backup data.

5.1.11 Trusted path (FPT)

5.1.11.1 Trusted path (FTP_TRP.1/TOE)

FTP_TRP.1.1/TOE: 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.

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

FTP_TRP.1.3/TOE The TSF shall require the use of the trusted path for initial user authentication /FIA_UID.1, FIA_UAU.1) and TSF management (FMT_MOF.1, FMT_MSA.1/ROLE, FMT_MSA.1/USER, FMT_MSA.1/VAD, FMT_MSA.2, FMT_MSA.3/CRYPTO_AUDIT, FMT_MTD.1/ACCESS, FMT_MTD.1/AUDIT, FMT_SMR.1)

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 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 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.

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

5.3.1.2 Protected audit trail storage (FAU_STG.1/ENVIRONMENT)

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

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

5.3.2 User data protection (FDP)

The client application shall provide the TOE signing function to its authorised end-user only and shall prevent unauthorised transmission and manipulation of DTBS representation to be signed by the TOE.

5.3.2.1 Subset access control (FDP_ACC.1/CLIENT)

FDP_ACC.1.1/ CLIENT The TSF shall enforce the Client application SFP on end-user, TOE signing function, use.

5.3.2.2 Security attribute based access control (FDP_ACF.1/CLIENT)

FDP_ACF.1.1/ CLIENT The TSF shall enforce the Client application SFP to objects based on authorisation for TOE signing function.

Application Note:
The security attribute “authorisation for TOE signing function” is assigned to end-users of the client application with two possible values:

(a) authorised to use TOE signing function,
(b) not authorised to use TOE signing function.

FDP_ACF.1.2/ CLIENT — The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: authorised end-user is allowed to use TOE signing function.

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

FDP_ACF.1.4/ CLIENT — The TSF shall explicitly deny access of subjects to objects based on the rule: non-authorised end-user is not allowed to use TOE signing function.

5.3.2.3 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1 — The TSF shall enforce the Client application SFP to be able to transmit user data in a manner protected from modification, deletion and insertion errors.

FDP_UIT.1.2 — The TSF shall be able to determine on receipt of user data, whether modification, deletion and insertion has occurred.

5.3.3 Identification and authentication (FIA)

The client application shall identify and authenticate its end-user for use of the TOE signing function.

5.3.3.1 Timing of authentication (FIA_UAU.1/CLIENT)

FIA_UAU.1.1/ CLIENT — The TSF shall allow [*assignment: list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

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

5.3.3.2 Timing of identification (FIA_UID.1/CLIENT)

FIA_UID.1.1/ CLIENT — The TSF shall allow [*assignment: list of TSF mediated actions*] on behalf of the user to be performed before the user is identified.

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

5.3.4 Protection of the TOE Security Functions (FPT)

5.3.4.1 Inter-TSF availability within a defined availability metric (FPT_ITA.1)

FPT_ITA.1.1 The TSF shall ensure the availability of backup data provided to a remote trusted IT product within a defined by the CSP availability metric given the following conditions restore of the current backup data.

5.3.5 Trusted path (FPT)

5.3.5.1 Trusted path (FTP_TRP.1/CLIENT)

FTP_TRP.1.1/ CLIENT 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.

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

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

Application note:
If TOE does not have a human user interface for authentication and management, the client application will provide this interface and a trusted path for the communication between the user and the TOE. The client application shall support the trusted path as one for the communication entity.

5.3.6 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_Recovery *Recovery procedures for the TOE*

The CSP shall define and apply recovery plans and procedures which allow a secure and timely recovery of the TOE operational state. These procedures shall ensure at least

(1) secure initialisation of new TOE devices replacing other TOE devices

(2) re-initialisation of TOE devices establishing the secure state by the TSF FPT_FLS.1 after detecting failures by the TSF FPT_AMT.1 and FPT_TST.1,

(3) integrity check of the TOE hardware, firmware and software and re-initialisation of TOE devices if the TOE indicates physical tampering by TSF FPT_PHP.2 and destroyed the plaintext SCP-SCD and other confidential secret and private keys by TSF FPT_PHP.3.

If the TOE support backup of the CSP-SCD, other user data and TSF data the CSP will ensure the availability of the backup data and the cryptographic quality, confidentiality and availability of the backup keys.

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 CSP-SCD and signatures. This includes

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

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

(3) the export of the CSP-SVD by the TOE and the securing the authenticity of the CSP-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 advanced electronic signatures of qualified certificates. 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 Objectives Mapping

Policy/Threat/Assumptions	Objectives
Policies	
P.Algorithms	O.CSP-CSD_Secure, O.Sign_Secure
Threats to be addressed by the TOE	
T.Bad_Init	O.Audit_CM, O.CSP-CSD_Secure, O.Control_Services, O.Protect_Exported_Data
T.Bad_SW_Load	O.Control_Services
T.CSP-SCD_Derive	O.CSP-CSD_Secure, O.Check_Operation, O.Phys_Protect, O.Sign_Secure
T.CSP-SCD_Disclose	O.CSP-CSD_Secure, O.Check_Operation, O.Sign_Secure
T.CSP-SCD_Distortion	O.Check_Operation, O.Detect_Attack, O.Error_Secure
T.Data_Manipul	O.Protect_Exported_Data
T.Defect	O.Backup, O.Check_Operation, O.Protect_Exported_Data
T.Malfunction	O.Check_Operation, O.Error_Secure
T.Management	O.Audit_CM, O.Control_Services, O.Protect_Exported_Data, O.User_Authentication
T.Misuse	O.Audit_CM, O.Control_Services, O.User_Authentication
T.Phys_Manipul	O.Backup, O.Detect_Attack, O.Error_Secure
T.Signature_Forgery	O.Sign_Secure

Threats to be addressed by the TOE environment	
T.Bad_Init	O.ENV_Application, O.ENV_Recovery, O.ENV_Secure_Init
T.Data_Manipul	O.ENV_Application, O.ENV_Secure_Oper
T.Defect	O.ENV_Backup, O.ENV_Protect_Access, O.ENV_Recovery
T.Insecure_Init	O.ENV_Application, O.ENV_Personnel, O.ENV_Protect_Access, O.ENV_Secure_Init
T.Insecure_Oper	O.ENV_Personnel, O.ENV_Protect_Access, O.ENV_Secure_Oper
T.Malfunction	O.ENV_Recovery
T.Phys_Manipul	O.ENV_Protect_Access
T.Theft	O.ENV_Protect_Access, O.ENV_Recovery, O.ENV_Secure_Oper
Assumptions	
A.Audit_Support	O.Audit_CM, O.ENV_Audit, O.ENV_Personnel
A.Correct_DTBS	O.ENV_Application, O.ENV_Human_Interface, O.ENV_Secure_Oper
A.Data_Store	O.ENV_Backup, O.ENV_Recovery
A.Human_Interface	O.ENV_Application, O.ENV_Human_Interface
A.User_Authentication	O.ENV_Human_Interface, O.ENV_Application, O.ENV_Secure_Init, O.ENV_Secure_Oper, O.User_Authentication
A.User_Management	O.ENV_Personnel, O.ENV_Secure_Init, O.ENV_Secure_Oper

Table 6-2 Tracing of Security Objectives to the TOE Security Environment

Objectives	Policy/Threat/Assumptions
Security Objectives for the TOE	
O.Audit_CM	A.Audit_Support, T.Bad_Init, T.Management, T.Misuse
O.Backup	T.Defect, T.Phys_Manipul
O.CSP-CSD_Secure	P.Algorithms, T.Bad_Init, T.CSP-SCD_Derive, T.CSP-SCD_Disclose
O.Check_Operation	T.CSP-SCD_Derive, T.CSP-SCD_Disclose, T.CSP-SCD_Distortion, T.Defect, T.Malfunction
O.Control_Services	T.Bad_Init, T.Bad_SW_Load, T.Management, T.Misuse
O.Detect_Attack	T.CSP-SCD_Distortion, T.Phys_Manipul
O.Error_Secure	T.CSP-SCD_Distortion, T.Malfunction, T.Phys_Manipul
O.Protect_Exported_Data	T.Bad_Init, T.Data_Manipul, T.Defect, T.Management
O.Sign_Secure	P.Algorithms, T.CSP-SCD_Derive, T.CSP-SCD_Disclose, T.Signature_Forgery
O.User_Authentication	A.User_Authentication, T.Management, T.Misuse
Security Objectives for the Environment	
O.ENV_Application	A.Correct_DTBS, A.Human_Interface, A.User_Authentication, T.Bad_Init, T.Data_Manipul, T.Insecure_Init
O.ENV_Audit	A.Audit_Support
O.ENV_Backup	A.Data_Store, T.Defect
O.ENV_Human_Interface	A.Correct_DTBS, A.Human_Interface, A.User_Authentication
O.ENV_Personnel	A.Audit_Support, A.User_Management, T.Insecure_Init, T.Insecure_Oper
O.ENV_Protect_Access	T.Defect, T.Insecure_Init, T.Insecure_Oper, T.Phys_Manipul, T.Theft
O.ENV_Recovery	A.Data_Store, T.Bad_Init, T.Defect, T.Malfunction, T.Theft

O.ENV_Secure_Init	A.User_Management, T.Bad_Init, T.Insecure_Init
O.ENV_Secure_Oper	A.Correct_DTBS, A.User_Authentication, A.User_Management, T.Data_Manipul, T.Insecure_Oper, T.Theft

6.2.2 Security Objectives Sufficiency

The overall objective of this Protection Profile is to provide a basis for cryptographic devices used within a CA environment to store and apply the private keys of a CA to sign certificates, certificate revocation lists, time stamp certificates or OCSP responses. Basic requirements for such a device are defined in the EU directive [1] as well as in the ETSI document on policy requirements for certification authorities issuing qualified certificates [6]. In addition the objectives of FIPS 140-2 for cryptographic modules have been taken into account.

In this chapter we will map the security objectives, threats and assumptions on the requirements stated in those documents to demonstrate compliance with the EU directive. In addition we will present the arguments for the consistency of the objectives, assumptions and threats defined.

6.2.2.1 Policies and Security Objective Sufficiency

P.Algorithms addresses the problem to use cryptographic algorithms and parameters that provide the required level of security against cryptographic attacks resulting in the ability to generate false signatures. These properties are addressed in the objectives O.CSP-SCD_Secure and O.Sign_Secure.

6.2.2.2 Threats and Security Objective Sufficiency

T.Bad_Init deals with the threat of a CSP signing device initiated in an insecure way. Each CSP signing device will need to be initialised correctly and in a secure way before it can be used within a CA environment for issuing and managing qualified certificates. Secure Initialisation includes the secure generation or import of the CA keys as well as the secure setup of the CSP signing device TSF management data. This threat is countered by O.CSP-SCD_Secure with respect to the secure CSP-SCD generation and management, O.Control_Services with respect to the unauthorised use of services (also in the initialisation phase) as well as by objectives on the TOE environment O.ENV_Secure_Init and O.ENV_Recovery. In addition O.Audit_CM provides the ability to check if the initialisation process has been performed correctly.

O.ENV_Recovery covers the case where a CSP signing device has to be initialised to take over the task of another CSP signing device e. g. in the case this device works incorrectly.

A TOE may also be initialised to be copy of another TOE that became unusable e. g. because of a hardware failure. In this case the TOE needs to be initialised with TSF data that has been previously exported from the other TOE. O.Protect_Exported_Data addresses the issue that this data has been manipulated after it has been exported. This allows the new TOE to get securely initialised with the data of the old TOE.

T.Bad_SW_Load deals with the threat of introducing potentially malicious or faulty code into the TOE after it has been checked and released for use. Not all CSP signing devices may provide a capability to modify the operational software in those stages of the life-cycle, but many CSP signing devices may provide the ability to install software updates. In this case O.Control_Services will ensure that only authorised users can perform such an update.

T.CSP-SCD_Derive deals with the threat that the CSP-SCD can be derived from the reaction and responses of the CSP signing device. This includes any type of covert storage channel which can be used to extract information about the CSP-SCD as well as the problem of timing channels or other signals of the CSP signing device that may carry information about the CSP-SCD. Examples are power consumptions or radiation.

O.CSP-SCD_Secure is responsible to ensure that no information about the CSP-SCD is directly transmitted to any entity outside the TOE. O.Phys_Protect ensures that attacks using physical probing are addressed. Leakage of information via e. g. the power consumption or via radiation may require sufficient physical protection of the CSP signing device in its operational environment, which is addressed by O.ENV_Protect_Access.

O.Sign_Secure ensures that the algorithms and the specific implementation will not reveal the CSP-SCD.

T.CSP-SCD_Disclose deals with the threat of disclosing directly all or part of the CSP-SCD via the defined interfaces. This may happen either because a defined function allows the unencrypted export of CSP-SCD, the CSP-SCD is not protected sufficiently when exported e. g. for backup or because of the incorrect operation of an element of the TOE. Unencrypted export of the CSP-SCD is prohibited by O.CSP-SCD_Secure, the protection of exported TOE data is addressed by O.Protect_Exported_Data and the incorrect operation is addressed by O.Check_Operation. In addition O.Sign_Secure ensures that the CSP-SCD is not disclosed as part of the signed data exported to the user.

T.CSP-SCD_Distortion deals with the threat that the CSP-SCD gets corrupted either by a software or hardware malfunction or by a deliberate physical attack on the TOE. This threat is only relevant, if the TOE will use the distorted CSP-SCD. Therefore it has to be the objective to detect the distortion of the CSP-SCD, not only to prevent such a distortion.

O.Check_Operation will ensure that the TOE will check the CSP-SCD regularly. O.Error_Secure will prevent the TOE to use distorted CSP-SCD after it has detected the distortion and O.Detect_Attack will prohibit the use of a distorted CSP-SCD after a physical attack (of course in the case of a physical attack the TOE will itself destroy the CSP-SCD and enter a state where it can only be reused after a secure re-initialisation).

T.Malfunction deals with the threat of malfunction of the TOE hardware. As a result the DTBS-representation, the CSP-SCD or TSF management data may be corrupted or the result of TOE operations may be false. As a consequence CSP-SCD may be disclosed or distorted data may be signed by the TOE. This threat is countered by O.Check_Operation and O.Error_Secure (which ensures that the TOE will not continue to operate with the CSP-SCD when it has detected a malfunction.

T.Management deals with the threat of misusing TOE management functions during initialisation and operation. The only way the TOE can deal with this threat is by restricting the

use of TOE management functions to users authorised to use those functions and by auditing the actions of those users. Therefore the threat is countered by O.Control_Services, which restricts the use of TOE management functions to authorised users, O.User_Authentication, which ensures that the invoking a management function has the authorisation and O.Audit_CM, which allows to trace the actions of those users. In addition the objective O.Protect_Exported_Data prohibits the modification of data exported by the TOE when it is imported again (which otherwise could be used to manipulate TSF management data).

T.Misuse deals with the threat of misuse of the TOE to create a forged signature. This could be achieved, if an unauthorised user could invoke the signature function. O.Control_Services counters this threat. O.User_Authentication prevents the misuse by persons not authorised to use the TOE and O.Audit_CM allows checking, if an unauthorised user has attempted to get access to the TOE or if an authorised user has attempted to misuse the TOE by attempting to use functions he is not allowed to use.

T.Phys_Manipul deals with physical manipulation of the TOE. An attacker may try to get access to the CSP-SCD by trying to get physical access to the location where it is stored. O.Detect_Attack counters this threat as long as the TOE is directly able to detect that it is under attack. O.Error_Secure counters the case where the TOE does not detect the physical manipulation directly but detects an error during operation that might have been caused y a physical attack.

Since it is obvious that the TOE is not able to withstand all kind of physical manipulation, O.ENV_Protect_Access shall prohibit (as far as possible) the likelihood that an attacker is able to perform any physical manipulation on the TOE.

T.Signature_Forgery deals with the threat that an attacker is able to generate a forged signature with the result that either a forged qualified signature or forged certificate status information is generated. While the threat of disclosing information about the CSP-SCD is covered elsewhere, this threat deals with the problem that it might be able for someone to forge a signature without knowledge of the CSP-SCD. O.Sign_Secure counters this threat by stating that it should not be possible to generate a valid signature without knowledge of the CSP-SCD.

T.Defect deals with the threat that a defect may prohibit the TOE to operate correctly. Examples of defects are faults within hardware components of the TOE, loss or corruption of programs and/or data within the TOE due to component failures or ageing, accidental or deliberate destruction of the TOE or its components. As a result the TOE is no longer able to generate a correct signature. Due to the criticality of the TOE and the requirement for resistance to physical attacks, maintenance of the TOE is also critical and repairing the TOE might be impossible without deleting the CSP-SCD. Therefore the TOE should be protected as far as possible from defects caused by deliberate or accidental mishandling (this is covered by the objective O.ENV_Protect_Access). On the other hand, if a defect occurs procedures within the TOE environment have to exist that allow the organisation operating the TOE to recover in a secure way from this defect. This is covered by the objective O.ENV_Recovery. This protection profile does not state specific details of the recovery procedure, because the requirements on this procedure depend on the overall requirements and architecture of the system where the TOE is used to sign qualified certificates or certificate status information. A recovery procedure may or may not include the secure recovery of the CSP-SCD or other TSF internal data. If the recovery of this information is required, this is covered by O.ENV_Backup. Backup data itself is protected by O.Protect_Exported_Data.

In addition the TOE objective O.Check_Operation ensures that the TOE is able to detect some defects itself and prohibits the use of the TOE with these defects.

T.Insecure_Init deals with threat that the TOE might be set up in an insecure way. This includes the generation or loading of the CSP-SCD, the initialisation of other TSF data like the definition of roles and initial access control conditions or the setup of the functions and parameters the TOE provides to external entities. Procedures within the TOE environment have to be in place that monitor the correct initialisation of the TOE before it is accepted to sign qualified certificates or certificate status information. To counter this threat, organisational controls shall be in place that verify the correct initialisation and protect the TOE before it is initialised. In addition, applications running on systems within the TOE environment have to perform the necessary checks within the initialisation procedure e. g. if those applications generate data that is then downloaded to the TOE and used there as TSF data. O.ENV_Protect_Access addresses the aspect of physical access to an un-initialised TOE by unauthorised personnel, O.ENV_Secure_Init covers addresses the organisational aspects while O.ENV_Application addresses the aspect of security checks and controls within the applications used in the TOE environment for the initialisation of the TOE. In addition, the personnel performing the initialisation actions must be aware of the implications of their activities and trained to perform their task correctly. This is covered by the objective O.ENV_Personnel

T.Insecure_Oper deals with the threat that the TOE might be operated in an insecure way and where the TOE itself is not able to detect this. This includes the possibility to operate the TOE in a hostile system that simulates the intended system environment or a valid system environment is operated without in violation of the requirements stated in the EU directive, national laws or regulations. This threat is addressed by the objective O.ENV_Secure_Oper. Physical protection of the TOE, which is also necessary to operate the TOE securely, is addressed by O.ENV_Protect_Access. In addition all personnel performing operational activities with the TOE or within the TOE environment must be aware of their duties and responsibilities and must be trained to perform their actions in accordance with the defined procedures. This is addressed by the objective O.ENV_Personnel.

T.Theft deals with the threat that the TOE might be stolen. A stolen TOE might be used within a hostile system environment (with the intent to generate valid signatures for false data), might be subject to strong physical attacks trying to reveal the CSP-SCD or just might be stolen to create a denial of service attack on the organisation using the TOE. It is the responsibility of the organisation using the TOE to prevent – as far as possible – theft of the TOE. If it happens anyhow, the organisation needs to have procedures in place to recover from the event as well as procedures to limit the damage that may happen if the thief tries to use the TOE within his environment or tries to extract the CSP-SCD from the TOE. This threat is therefore covered by the objectives O.ENV_Protect_Access (which tries to prevent theft), O.ENV_Recovery (which tries to limit the effect of the theft) and O.ENV_Secure_Oper, which limits the damage a thief can achieve by misuse of the TOE.

T.Data_Manipul deals with the threat that data to be signed is manipulated before it is submitted to the TOE. As a result the TOE may sign false certificates or certificate status information. This threat does not address manipulations the TOE is able to detect (e. g. data protected by secure checksums or digital signatures). Instead it addresses the threat of false data to be signed generated by those system components that are allowed to generate data to be signed. An example is a Registration Authority where an authorised operator has made a mistake in defining the certificate content data. Another example is a directory service

generating wrong certificate status information which is then submitted to the TOE for signing. This threat has to address in the TOE environment by the objective O.ENV_Secure_Oper and O.ENV_Application.

6.2.2.3 Assumptions and Security Objective Sufficiency

A.Audit_Support is addressed by the objectives O.Audit_CM, which ensures that all relevant events are audited and exported by the TOE and O.ENV_Audit, which ensures that the audit trail is properly analysed. The personnel performing this analysis must be aware of their duties and responsibilities, which is addressed by the objective O.ENV_Personnel.

A.Correct_DTBS is addressed by the objective O.ENV_Human_Interface, which ensures that the direct communication between human users and the TOE is integrity protected. O_ENV_Application ensures that the applications that use the TOE will perform the required checks on the data they pass to the TOE. O.ENV_Secure_Oper ensures that the necessary operational procedures are in place for the organisation operating the TOE as part of their certification system. With the sum of these objectives the assumption is covered.

A.Data_Store is addressed by the objective O.ENV_Backup, which deals with the security of backup data stored in the TOE environment. In addition O.ENV_Recovery addresses the availability of data stored in the TOE environment.

A.Human_Interface is addressed by the objective O.ENV_Human_Interface and the objective O.ENV_Application.

A.User_Authentication is addressed by the TOE objective O.User_Authentication as well as the objectives O.ENV_Application and O.ENV_Secure_Oper with respect to the TOE environment. The objective O.User_Authentication addresses users that directly authenticate to the TOE as individual users. O.ENV_Application and O.ENV_Secure_Oper address the problem where the authentication of an individual user is performed outside of the TOE (e. g. within the system of a registration authority) and the TOE only performs role-based authentication.

A.User_Management is addressed by the objectives O.ENV_Secure_Init and O.ENV_Secure_Oper. O.ENV_Secure_Init addresses the secure initial set-up of the users and roles for the TOE and O.ENV_Secure_Oper addresses the aspect of the procedures to manage the TOE users outside of the TOE. This assumption is required, because the TOE is not required to maintain all users with the role of Crypto-user itself. Instead individual Crypto-users may be maintained by other entities (e. g. a Registration Authority) where the TOE is only able to identify and authenticate that a legitimate user of that other entity has called for a TOE function, but is not able to associate an identity with this user. In this case, appropriate management procedures for the management of those users have to be in place, which is covered by the objective O.ENV_Secure_Oper. Personnel performing user management activities must be aware of their responsibilities and duties, which is addressed by the objective O.ENV_Personnel.

6.3 Security Requirements Rationale

6.3.1 Security Requirement Coverage

Table 6-3 Functional and Assurance Requirement to Security Objective Mapping

Objectives	Requirements
Security Objectives for the TOE	
O.Audit_CM	FAU_GEN.1/BASIC, FAU_GEN.2/BASIC, FAU_STG.2/TOE, FDP_ACC.1/AUDIT, FDP_ACF.1/AUDIT, FMT_MTD.1/AUDIT, FPT_ITI.1 Backup Package: FAU_GEN.1/BACKUP, FAU_GEN.2/BACKUP
O.Backup	Backup package: FAU_GEN.1/BACKUP, FAU_GEN.2/BACKUP, FCS_CKM.2/BACKUP, FCS_COP.1/BACKUP_ENC, FCS_COP.1/BACKUP_INT, FDP_ACC.1/BACKUP, FDP_ACF.1/BACKUP, FDP_BKP.1, FDP_IFC.1/BACKUP, FDP_IFF.4/BACKUP, FMT_MSA.1/BACKUP_ROLE, FMT_MSA.1/BACKUP_USER, FMT_MSA.1/BACKUP_VAD, FMT_MSA.3/BACKUP, FPT_ITC.1, FPT_ITI.1
O.CSP-CSD_Secure	FCS_CKM.1, FCS_CKM.4, FCS_COP.1/SIGN, FDP_ACC.1/CRYPTO, FDP_ACF.1/CRYPTO, FDP_IFC.1/CRYPTO, FDP_ETC_KEY.1, FDP_IFF.4/CRYPTO, FDP_RIP.1, FDP_SDI.2, FIA_SOS.2
O.Check_Operation	FPT_TST.1, FPT_AMT.1
O.Control_Services	FDP_ACC.1/CRYPTO, FDP_ACC.1/AUDIT, FDP_ACF.1/CRYPTO, FDP_ACF.1/AUDIT, FMT_MSA.1/ROLE, FMT_MSA.2, FMT_MSA.3/CRYPTO_AUDIT, FMT_MTD.1/AUDIT, FMT_MTD.1/ACCESS_CONTROL, FMT_SMR.1 Backup package: FDP_ACC.1/BACKUP, FDP_ACF.1/BACKUP, FMT_MSA.1/BACKUP_ROLE, FMT_MSA.3/BACKUP
O.Detect_Attack	FPT_PHP.2, FPT_PHP.3
O.Error_Secure	FPT_AMT.1, FPT_FLS.1, FPT_RCV.1, FPT_TST.1
O.Protect_Exported_Data	FDP_BKP.1, FCS_COP.1/BACKUP_ENC, FCS_COP.1/BACKUP_INT, FDP_ETC.1, FDP_ETC_KEY.1
O.Sign_Secure	FCS_CKM.1, FCS_COP.1/SIGN, FDP_IFC.1/CRYPTO, FDP_IFF.4/CRYPTO

Objectives	Requirements
O.User_Authentication	FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.1, FIA_UID.1, FMT_MSA.1/USER, FMT_MSA.1/VAD Backup package: FMT_MSA.1/BACKUP_USER, FMT_MSA.1/BACKUP_VAD,
Security Objectives for the Environment	
O.ENV_Application	FIA_UID.1/CLIENT, FIA_UAU.1/CLIENT, FDP_ACC.1/CLIENT, FDP_ACF.1/CLIENT, FDP_UIT.1
O.ENV_Audit	FAU_SAR.1, FAU_STG.1/ENVIRONMENT,
O.ENV_Backup	FPT_ITA.1
O.ENV_Human_Interface	FTP_TRP.1
O.ENV_Personnel	RE.ENV_Personnel
O.ENV_Protect_Access	RE.ENV_Protect_Access
O.ENV_Recovery	RE.ENV_Recovery
O.ENV_Secure_Init	RE.ENV_Secure_Init
O.ENV_Secure_Oper	RE.ENV_Secure_Oper
Security Assurance Requirements	
O.Backup	ADV_IMP.2, AVA_CCA.1
O.CSP-SCD_Secure	ADV_IMP.2, AVA_CCA.1, AVA_VLA.4
O.Protect_Exported_Data	AVA_VLA.4
O.Sign_Secure	AVA_CCA.1, AVA_VLA.4
Security Objectives	ACM_AUT.1, ACM_CAP.4, ACM_SCP.2, ADO_DEL.2, ADO_IGS.1, ADV_FSP.2, ADV_HLD.2, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1, AGD_ADM.1, AGD_USR.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, AVA_MSU.2, AVA_SOF.1, AVA_VLA.4

6.3.2 Security Requirements Sufficiency

6.3.2.1 TOE Security Requirements Sufficiency

O.Audit_CM (Audit record generation and export) addresses the generation and protection of audit data by the TOE. The audit generation is implemented by the SFR FAU_GEN.1/BASIC and FAU_GEN.2/BASIC with the audit events matching the list in O.Audit_CM. Additional audit is implemented by the SFR FAU_GEN.1/BACKUP and FAU_GEN.2/BACKUP if backup is

supported by the TOE. The TOE stores the audit data according to the SFR FAU_STG.2/TOE until the audit trail is exported upon request of the Crypto-officer under control of the SFR FDP_ACC.1/AUDIT, FDP_ACF.1/AUDIT and FMT_MTD.1/AUDIT. The integrity of the audit data will be ensured by the SFR FAU_STG.2/TOE inside the TOE and by the SFR FPT_ITI.1 in the TOE environment.

O.Backup (Backup and restore for TOE) addresses the protection of the confidentiality and the detection of the integrity loss of the backup data if the TOE supports backup and restore. Because backup and restore is optional the additional SFR are collected in the backup package (refer to sections 5.1.7 to 5.1.10). The backup and restore of CSP-SCD, other user data and TSF data is described in the SFR FDP_BKP.1. The confidentiality and integrity protection of the TSF data as part of the backup data is implemented by the SFR FPT_ITC.1 and SFR FPT_ITI.1 The FDP_BKP.1 needs the cryptographic functions implemented by the following SFR: (i) import the backup keys by FCS_CKM.2/BACKUP, (ii) encryption of backup data by FCS_COP.1/BACKUP_ENC, (iii) data integrity protection by FCS_COP.1/BACKUP_INT. The backup and restore TSF will be under access control required by the SFR FDP_ACF.1/BACKUP according to FDP_ACC.1/BACKUP. The SFR FMT_MSA.1/BACKUP_ROLE, FMT_MSA.1/BACKUP_USER, FMT_MSA.1/BACKUP_VAD and FMT_MSA.3/BACKUP extend the management functions of security attributes to the Backup SFP. The SFR FAU_GEN.1/BACKUP and FAU_GEN.2/BACKUP require additional audit data specific for the backup and restore function. Because FDP_BKP.1 handles and exports the CSP-SCD outside the TSC the TOE shall protect against side-channels to prevent any illicit information flow. The SFR FDP_IFC.1/BACKUP and FDP_IFF.4/BACKUP implements this protection and the SFR AVA_CCA.1 requires subject side-channels to the vulnerability analysis.

O.CSCD_Secure (secure CSP-SCD generation and management) addresses the confidentiality and integrity of the CSP-SCD which shall be ensured during their whole life time. The SFR ensure the cryptographic secure CSP-SCD generation by FCS_CKM.1 and FIA_SOS.2 as well as operation by FCS_COP.1/SIGN according to the list of approved algorithms and parameters. The confidentiality and integrity of the CSP-SCD will be protected by SFR FDP_RIP.1 and FDP_SDI.2 while internal processing. The SFR FDP_ETC_KEY.1 will protect the confidentiality if the CSP-SCD (or any other cryptographic key) is exported. The SFR FCS_CKM.4 requires secure key destruction to prevent any misuse of CSP-SCD after operational life time. The all CSP-SCD management and operation is under access control of the SFR FDP_ACC.1/CRYPTO and FDP_ACF.1/CRYPTO. The TOE shall protect CSP-SCD against side-channels by the SFR FDP_IFC.1/CRYPTO and FDP_IFF.4/CRYPTO. The SAR AVA_CCA.1 requires subject side-channels to the vulnerability analysis. Note that the special protection of the CSP-SCD needed in case of the optional backup and restore is addressed by O.Backup and implemented by appropriate SFR (see above). The complex protection of the CSP-SCD as most valuable asset requires a systematic and complete vulnerability analysis considering high attack potential by SAR AVA_VLA.4.

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 for abstract machine testing FPT_AMT.1 and TSF testing FPT_TST.1. 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_Servcies (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:

a) FDP_ACC.1/CRYPTO and FDP_ACF.1/CRYPTO for the cryptographic functions (Crypto-SFP),

b) FDP_ACC.1/AUDIT and FDP_ACF.1/AUDIT for the audit function (Audit-SFP),

c) FDP_ACC.1/BACKUP and FDP_ACF.1/BACKUP for the backup function (Backup-SFP) if backup is supported by the TOE

with the roles Crypto-officer and Crypto-user as defined by the SFR FMT_SMR.1. The SFR FMT_MSA.1/ROLE, FMT_MSA.2, FMT_MSA.3/CRYPTO_AUDIT, FMT_MTD.1/ACCESS_CONTROL and FMT_MTD.1/AUDIT assign the management functions for the cryptographic and audit functions to the Crypto-officer. The SFR FMT_MSA.1/BACKUP_ROLE and FMT_MSA.3/BACKUP extend the Crypto-officer's management functions to backup if backup is supported by the TOE. The SFR require the TSF to enforce the Crypto-SFP and Audit-SFP (and Backup-SFP if backup is supported) to provide restrictive default values for security attributes which may be changed by the Crypto-officer. Note that the user management is addressed by O.User_authentication.

O.Detect_Attack (detection of physical attacks) addresses the detection of physical tampering attempts and the secure destruction of the CSP-SCD if such attempts are detected. The SFR FPT_PHP.2 implements notification of and FPT_PHP.3 resistance to physical attack. 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 CSP-SCD confidentiality whenever the TOE detects an error. The SFR FPT_AMT.1 and FPT_TST.1 require tests for error detection and the SFR FPT_FLS.1 requires preservation of a secure state when errors are detected. The TSF shall destroy the plaintext SCP-SCD and other confidential secret and private keys if failures occur. The SFR FPT_RCV.1 requires a maintenance mode where the ability to return the TOE to a secure state is provided. Note that the RE.ENV_Recovery describes the related security measures in the TOE environment.

O.Protect_Exported_Data (protection of TSF data exported by the TOE) addresses the integrity and confidentiality protection measures to all assets listed in the asset list requiring integrity or confidentiality protection when they are exported from the TOE. The SFR FDP_ETC.1 implements the Crypto-SFP and Audit SFP for all exported data. The SFR FDP_ETC_KEY.1 requires encrypting the CSP-SCD and electronically exported keys if they are exported (even if general backup is not supported by the TOE). If the TOE supports backup and restore functions the SFR FDP_BKP.1 requires the confidentiality and integrity protection of backup data. The cryptographic function shall be implemented according to FCS_COP.1/BACKUP_ENC and FCS_COP.1/BACKUP_INT.

O.Sign_Secure (Secure advanced signature-creation) addresses the security of the signatures, i.e. the signature does not reveal the CSP-SCD and cannot be forged without knowledge of the CSP-SCD. The cryptographic security of signature is implemented by the SFR FCS_CKM.1 and FCS_COP.1/SIGN with reference to the list of approved algorithms and parameters [5]. The SFR FDP_IFC.1/CRYPTO and FDP_IFF.4/CRYPTO requires TSF to

prevent illicit information flow about the CSP-SCD through side-channels in the signatures. The SAR AVA_CCA.1 and AVA_VLA.4 requires covert-channel analysis and a systematic and complete vulnerability analysis considering high attack potential. That is because the signature-creation with CSP-SCD especially for certificates is the most important and critical service of the TOE.

O.User_authentication (authentication of users interacting with the TOE) addresses the identification and authentication the users before having any access to TOE protected assets. The SFR require timing identification by FIA_UID.1 and timing authentication by FIA_UAU.1. 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 defines the security attributes for identity based authentication. Note that the client application might be the only user in the Crypto-user role and may act as agent for several end-users in the TOE environment (see O.ENV_Application). The SFR FIA_SOS.1 ensures the verification of the quality of the secret used for authentication. The SFR FIA_AFL.1 protects the VAD against guessing. The SFR FMT_MSA.1/USER and FMT_MSA.1/VAD provides management functions for identification and authentication in the basic package which are extended by FMT_MSA.1/BACKUP_USER and FMT_MSA.1/BACKUP_VAD if the TOE supports backup and restore.

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 signing function provided and passes the DTBS representation to the TOE. The client application shall implement end-user identification and authentication required by the SFR FIA_UID.1/CLIENTand FIA_UAU.1/CLIENT. It shall implement access control for the DTBS representation sent to the TOE for signing according to the SFR FDP_ACC.1/CLIENT and FDP_ACF.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.

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. Because the TOE implements access control on reading the TOE's audit trail only the SFR FAU_STG.1/ENVIRONMENT ensures the availability of the TOE audit trail and prevents the modification of the TOE audit trail outside the TOE.

O.ENV_Backup (secure handling of backup media) addresses the availability of the backup data in the case a restore is required. This is implemented in the IT environment by the SFR FPT_ITA.1. Note that the confidentiality and integrity of the backup data is addressed by the security objective O.Backup of the TOE.

O.ENV_human_interface (reliable human interface) addresses the confidentiality and integrity of the data transferred between the TOE and the human user if the client application provides a human interface and a communication path between human users and the TOE. In this case the client application will implement the trusted path according to SFR FTP_TRP.1 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 physical and logical protection of the TOE, the restriction the TOE usage and the limitation of the access to TOE assets to authorised persons only. The RE.ENV_Protect_Access requests the CSP to establish physical and organisational security measures 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. Note that the TOE itself protects by FPT_PHP.2 and FPT_PHP.3 the confidentiality of the CSP-SCD against physical access because even the CSP personnel do not need to know the CSP-SCD in plaintext.

O.ENV_Recovery (Secure Recovery in Case of Major Failure) addresses the recovery plans and procedures for a secure and timely recovery in the case of a major problem with the TOE. The RE.ENV_Recovery implements such recovery plans and procedures using the TOE TSF according to FDP_BKP.1 and other SFR. It takes recovery in case of detected errors or physical tampering into account.

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 CSP-SCD and initialisation of the signature function.

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.

6.4 Dependency Rationale

6.4.1 Functional and Assurance Requirements Dependencies

Table 6.4 Functional and Assurance Requirements Dependencies

Requirement	Dependencies	Remark
Functional Requirements		
FAU_GEN.1/BACKUP	-	Relevant for the backup package only
FAU_GEN.1/BASIC	-	
FAU_GEN.2/BACKUP	FAU_GEN.1/BACKUP, FIA_UID.1	Relevant for the backup package only
FAU_GEN.2/BASIC	FAU_GEN.1/BASIC, FIA_UID.1	
FAU_SAR.1	FAU_GEN.1/BASIC	
FAU_STG.1/ ENVIRONMENT	FAU_GEN.1/BASIC, FAU_GEN.1/BACKUP	The TOE environment stores the audit trails of the TOE. FAU_GEN.1/BACKUP is relevant for the backup package only.
FAU_STG.2/TOE	FAU_GEN.1/BASIC, FAU_GEN.1/BACKUP	FAU_GEN.1/BACKUP is relevant for the backup package only.
FCS_CKM.1	FCS_COP.1/SIGN, FCS_CKM.4, FMT_MSA.2 FCS_CKM.2/BACKUP	FCS_CKM.2/BACKUP is relevant for the backup package only.
FCS_CKM.2/ BACKUP	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Relevant for the backup package only
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2	
FCS_COP.1/ BACKUP_ENC	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Relevant for the backup package only
FCS_COP.1/ BACKUP_INT	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Relevant for the backup package only
FCS_COP.1/SIGN	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	

Requirement	Dependencies	Remark
FDP_ACC.1/BACKUP	FDP_ACF.1/BACKUP	Relevant for the backup package only
FDP_ACC.1/AUDIT	FDP_ACF.1/AUDIT	
FDP_ACC.1/CRYPTO	FDP_ACF.1/CRYPTO	
FDP_ACF.1/BACKUP	FDP_ACC.1/BACKUP, FMT_MSA.3/BACKUP	Relevant for the backup package only
FDP_ACF.1/AUDIT	FDP_ACC.1/AUDIT, FMT_MSA.3/CRYPTO_AUDIT	
FDP_ACF.1/CRYPTO	FDP_ACC.1/CRYPTO, FMT_MSA.3/CRYPTO_AUDIT	
FDP_BKP.1	FCS_CKM.2/BACKUP, FCS_COP.1/BACKUP_ENC, FCS_COP.1/BACKUP_INT	Relevant for the backup package only
FDP_ETC.1	FDP_ACC.1/CRYPTO, FDP_ACC.1/BACKUP, FDP_ACC.1/AUDIT, FDP_IFC.1/CRYPTO, FDP_IFC.1/BACKUP	
FDP_ETC_KEY.1	-	
FDP_IFC.1/BACKUP	-	Relevant for the backup package only
FDP_IFC.1/CRYPTO	-	
FDP_IFF.4/BACKUP	AVA_CCA.1, FDP_IFC.1/BACKUP	Relevant for the backup package only
FDP_IFF.4/CRYPTO	AVA_CCA.1, FDP_IFC.1/CRYPTO	
FDP_UIT.1	No detailed requirements for the TOE environment	
FIA_AFL.1	FIA_UAU.1	
FIA_UAU.1	FIA_UID.1	
FMT_MSA.1/USER	FDP_ACC.1/CRYPTO, FDP_IFC.1/AUDIT, FMT_SMR.1	

Requirement	Dependencies	Remark
FMT_MSA.1/VAD	FDP_ACC.1/CRYPTO, FDP_IFC.1/AUDIT, FMT_SMR.1	
FMT_MSA.1/ BACKUP_ROLE	FDP_ACC.1/BACKUP, FMT_SMR.1	Relevant for the backup package only
FMT_MSA.1/ BACKUP_USER	FDP_ACC.1/BACKUP, FMT_SMR.1	Relevant for the backup package only
FMT_MSA.1/ BACKUP_VAD	FDP_ACC.1/BACKUP, FMT_SMR.1	Relevant for the backup package only
FMT_MSA.1/ROLE	FDP_ACC.1/CRYPTO, FDP_IFC.1/AUDIT, FMT_SMR.1	
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1/AUDIT, FDP_IFC.1/CRYPTO, FMT_MSA.1/ ROLE, FMT_MSA.1/BACKUP_ROLE, FMT_SMR.1	
FMT_MSA.3/ BACKUP	FMT_MSA.1/BACKUP_ROLE, FMT_MSA.1/BACKUP_USER, FMT_SMR.1	Relevant for the backup package only
FMT_MSA.3/ CRYPTO_AUDIT	FMT_MSA.1/ROLE, FMT_MSA.1/USER, FMT_MSA.1/VAD, FMT_SMR.1	
FMT_MTD.1/AUDIT	FMT_SMR.1	
FMT_MTD.1/ ACCESS_CONTROL	FMT_SMR.1	
FMT_SMR.1	FIA_UID.1	
FPT_FLS.1	ADV_SPM.1	
FPT_ITC.1	-	
FPT_ITI.1	-	
FPT_PHP.2	-	
FPT_RCV.1	FPT_TST.1, AGD_ADM.1, ADV_SPM.1	
FPT_TST.1	FPT_AMT.1	

Requirement	Dependencies	Remark
Assurance Requirements		
ACM_AUT.1	ACM_CAP.3	
ACM_CAP.4	ACM_SCP.1, ALC_DVS.1	
ACM_SCP.2	ACM_CAP.3	
ADO_DEL.2	ACM_CAP.3	
ADO_IGS.1	AGD_ADM.1	
ADV_FSP.2	ADV_RCR.1	
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1	
ADV_IMP.2	ADV_LLD.1, ADV_RCR.1, ALC_TAT.1	
ADV_LLD.1	ADV_HLD.2, ADV_RCR.1	
ADV_SPM.1	ADV_FSP.1	
AGD_ADM.1	ADV_FSP.1	
AGD_USR.1	ADV_FSP.1	
ALC_TAT.1	ADV_IMP.1	ADV_IMP.2 is included and hierarchical to ADV_IMP.1
ATE_COV.2	ADV_FSP.1, ATE_FUN.1	
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1	
ATE_IND.2	ADV_FSP.1, AGD_ADM.1, AGD_USR.1, ATE_FUN.1	
AVA_CCA.1	ADV_FSP.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	
AVA_VLA.4	ADV_FSP.1, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, AGD_ADM.1, AGD_USR.1	ADV_IMP.2 is included and hierarchical to ADV_IMP.1

6.4.2 Justification of Unsupported Dependencies

Component	Justification for not including	
Security Functional Requirements		
FPT_PHP.2	FMT_MOF.1	FPT_PHP.2 informs the local user about detected tampering attempt. No management of security functions behaviour is needed.
FDP_IFC.1/CRYPTO	FDP_IFF.1	FDP_IFC.1/CRYPTO is defined for the CSP-SCD without reference to any security attribute.
FAU_GEN.1/BASIC	FPT_STM.1	FAU_GEN.1/BASIC 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 note directs the ST editor to include FPT_STM.1 if reliable time stamp is used by the TOE.
FAU_GEN.1/BACKUP	FPT_STM.1/BACKUP	FAU_GEN.1/Backup 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 note 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	FDP_IFC.1/CRYPTO is defined for the CSP-SCD without reference to any security attribute. The PP uses FDP_IFF.4/CRYPTO instead of FDP_IFF.1.
FDP_IFC.1/BACKUP	FDP_IFF.1	FDP_IFC.1/Backup is defined for the CSP-SCD without reference to any security attribute. The PP uses FDP_IFF.4/BACKUP instead of FDP_IFF.1.

6.5 - Security Functional Requirements Grounding in Objectives

Table 6-5 Requirements to Objectives 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	O.CSP-SCD_Secure, ADV_IMP.2 is hierarchical to ADV_IMP.1 required for EAL4
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

Requirement	Security Objectives
ATE_IND.2	EAL4
AVA_CCA.1	O.Sign_Secure, O.Backup, O.CSP-CSD_Secure
AVA_MSU.2	EAL4
AVA_SOF.1	EAL4
AVA_VLA.4	O.CSP-CSD_Secure, O.Protect_Exported_Data, O.Sign_Secure,
FAU_GEN.1/BACKUP	O.Audit_CM, O.Backup
FAU_GEN.1/BASIC	O.Audit_CM
FAU_GEN.2/BACKUP	O.Audit_CM, O.Backup
FAU_GEN.2/BASIC	O.Audit_CM
FAU_STG.2/TOE	O.Audit_CM
FCS_CKM.1	O.CSP-CSD_Secure, O.Sign_Secure
FCS_CKM.2/ BACKUP	O.Backup
FCS_CKM.4	O.CSP-CSD_Secure
FCS_COP.1/BACKUP _ENC	O.Protect_Exported_Data, O.Backup
FCS_COP.1/BACKUP _INT	O.Backup, O.Protect_Exported_Data
FCS_COP.1/SIGN	O.Sign_Secure, O.CSP-CSD_Secure
FDP_ACC.1/BACKUP	O.Backup, O.Control_Services
FDP_ACC.1/AUDIT	O.Audit_CM
FDP_ACC.1/CRYPTO	O.CSP-CSD_Secure, O.Control_Services
FDP_ACF.1/BACKUP	O.Backup, O.Control_Services
FDP_ACF.1/AUDIT	O.Control_Services, O.Audit_CM
FDP_ACF.1/CRYPTO	O.CSP-CSD_Secure, O.Control_Services

Requirement	Security Objectives
FDP_BKP.1	O.Backup, O.Protect_Exported_Data
FDP_ETC.1	O.Protect_Exported_Data
FDP_ETC_KEY.1	O.CSP-CSD_Secure
FDP_IFC.1/BACKUP	O.Backup, O.CSP-CSD_Secure
FDP_IFC.1/CRYPTO	O.CSP-CSD_Secure, O.Sign_Secure
FDP_IFF.4/BACKUP	O.Backup, O.CSP-CSD_Secure
FDP_IFF.4/CRYPTO	O.CSP-CSD_Secure, O.Sign_Secure
FDP_RIP.1	O.CSP-CSD_Secure
FDP_SDI.2	O.CSP-CSD_Secure
FIA_AFL.1	O.User_Authentication
FIA_ATD.1	O.User_Authentication
FIA_SOS.1	O.User_Authentication
FIA_SOS.2	O.CSP-CSD_Secure
FIA_UAU.1	O.User_Authentication
FIA_UID.1	O.User_Authentication
FMT_MSA.1/USER	O.User_Authentication
FMT_MSA.1/VAD	O.User_Authentication
FMT_MSA.1/ BACKUP_ROLE	O.Backup, O.Control_Services
FMT_MSA.1/ BACKUP_USER	O.Backup, O.User_Authentication
FMT_MSA.1/ BACKUP_VAD	O.Backup, O.User_Authentication
FMT_MSA.1/ROLE	O.Control_Services
FMT_MSA.2	O.Control_Services

Requirement	Security Objectives
FMT_MSA.3/BACKUP	O.Backup
FMT_MSA.3/ CRYPTO_AUDIT	O.Control_Services
FMT_MTD.1/AUDIT	O.Audit_CM
FMT_MTD.1/ ACCESS_CONTROL	O.Control_Services
FMT_SMR.1	O.Control_Services
FPT_AMT.1	O.Check_Operation, O.Error_Secure
FPT_FLS.1	O.Error_Secure
FPT_PHP.2	O.Detect_Attack
FPT_PHP.3	O.Detect_Attack
FPT_RCV.1	O.Error_Secure
FPT_TST.1	O.Error_Secure, O.Check_Operation
Security Objectives for the Environment	
FAU_SAR.1	O.ENV_Audit
FAU_STG.1/ ENVIRONMENT	O.ENV_Audit
FDP_UIT.1	O.ENV_Application
FPT_ITA.1	O.ENV_Backup
FPT_PHP.3	O.ENV_Protect_Access
FTP_TRP.1	O.ENV_Human_Interface

6.5 Rationale for Extensions

6.5.1 Rationale for Extension of Class FDP with Family FDP_BKP

The HSM may optional backup CSP-SCD, other user data and TSF data to restore the operational state of the same HSM or for a new HSM in the event of a system failure or other serious error. The export, import and protection of the backup data are combined in a specific

way. The HSM ensures the confidentiality of the backup data and detects loss of the integrity of the backup data. The availability of the backup data will be ensured by the TOE environment.

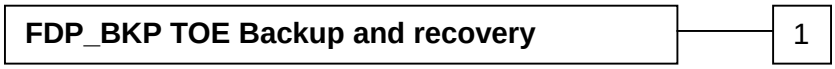
This component is necessary to specify a unique requirement of certificate issuing and management components that is not addressed by the Common Criteria.

Backup and recovery (FDP_BKP)

Family behaviour

This family defines export and import of the backup data. The TOE ensures the confidentiality of the backup data and detects loss of the integrity of the backup data. The availability of the backup data will be ensured by the TOE environment.

Component levelling:



FDP_BKP.1 Backup and recovery provides export, import and protection of the backup data.

Management: FDP_BKP.1

There are no management activities foreseen.

Audit: FDP_BKP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Use of the backup function,

b) Use of the recovery function,

c) Unsuccessful recovery because of detection of modification of the backup data.

FDP_BKP.1 Backup and recovery

Hierarchical to: No other components.

FDP_BKP.1.1 The TSF shall include a backup function.

FDP_BKP.1.2 The Crypto-officer shall be capable of invoking the backup function on demand.

FDP_BKP.1.3 The data stored in the backup shall be sufficient to recreate the state of the TOE at the time the backup was created using only:
(1) a copy of the same version of the TOE as was used to create the backup data;
(2) a stored copy of the backup data;
(3) the cryptographic key(s) needed to decrypt the CSP-SCD and any

other encrypted critical security parameters;
(4) the cryptographic key(s) needed to verify the cryptographic checksum of the backup data.

FDP_BKP.1.4 The TSF shall include a recovery function that is able to restore the state of the TOE from a backup.

FDP_BKP.1.5 The CSP-SCD, other critical security parameters and other confidential information shall be stored in encrypted form only.

FDP_BKP.1.6 The backup data shall be checked for modification through the use of cryptographic checksums. Modified backup data shall not be used for recovery.

Dependencies: [FCS_CKM.1 Cryptographic key generation
or
FCS_CKM.2 Cryptographic key distribution
or
FDP_ITC.1 Import of user data without security attributes]
FCS_COP.1 Cryptographic operation

6.5.2 Rationale for Extension of Class FDP with Family FDP_ETC_KEY

The TOE may export the CSP-SCD or other secret and private keys. The TOE shall protect the confidentiality of these keys independent of any optional backup function (see FDP_BKP.1). The component FDP_ETC_KEY.1 is required to specify a unique requirement for cryptographic trustworthy systems of the CSP that is not addressed by the Common Criteria.

Extended user private and secret key export (FDP_ETC_KEY)

Family behaviour

This family defines export of the CSP-SCD, secret and private keys to ensure their confidentiality.

FDP_ETC_KEY Extended user private and secret key export	1

Component levelling:

FDP_ETC_KEY.1 Extended user private and secret key export provides export and protection of the CSP-SCD, secret and private keys.

Management: FDP_ETC_KEY.1

There are no management activities foreseen.

Audit: FDP_ETC_KEY.1

There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

FDP_ETC_KEY.1 Extended user private and secret key export

Hierarchical to: No other components.

FDP_ETC_KEY.1.1 CSP-SCD shall only be exported from the TOE in encrypted form.

FDP_ETC_KEY.1.2 Secret keys and private keys other than CSP-SCD shall be exported from the TOE in encrypted form or using split knowledge procedures. Electronically distributed secret or private keys shall be exported from the TOE in encrypted form.

Dependencies: No dependencies

6.6 Rationale for Assurance Level 4 Augmented

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

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

The security objective O.CSP-SCD_Secure includes protection against disclosing completely or partly the CSP-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 CSP – the CSP-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] International Organization for Standardization, ISO/IEC 15408-1:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, 1999.

[3] International Organization for Standardization, *ISO/IEC 15408-2:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999.

[4] International Organization for Standardization, *ISO/IEC 15408-3:1999 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999.

[5] Algorithms and Parameters for Secure Electronic Signatures, 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] CEN/ISSS WS/E-Sign; Area D1, CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures

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

Appendix B (Informative)

Implementation Guidelines for Roles: Mapping the security requirements of this PP to a cryptographic module implementing PKCS#11

1. Introduction

Many cryptographic modules implement the cryptographic token interface defined in the PKCS#11 standard. It is the clear intention of this Protection Profile to allow such hardware based cryptographic modules to be compliant with the requirements of this PP. This informative annex will provide some guidance how this can be achieved. The basis for this analysis is version 2.10 of PKCS#11 (published December 1999). In addition draft 1 of version 2.11 (as published November 2000) has also been considered to avoid suggestions that are not compliant with the foreseeable future development of PKCS#11.

PKCS#11 has been defined as a general purpose interface for cryptographic modules for many different application scenarios. This includes, but is not limited to, the application of the cryptographic module within a CA environment. On the other hand this Protection Profile solely addresses the use of the cryptographic module within a CA environment for the signing of certificates and certificate status information. As a result the operational models underlying PKCS#11 and this Protection Profile are different and it is not obvious if and how they can be mapped. This informative annex will provide some guidance and suggestions how such a mapping may look like thereby suggesting additional functions to those required by PKCS#11 in order to satisfy the security requirements of this PP.

Reading PKCS#11 one could also think of using the Secondary Authentication mechanism to model the roles of this Protection Profile. However, since the chapter on Secondary Authentication has been deprecated in draft 1 of Version 2.11 of PKCS#11, this mechanism is not proposed to be used.

Differences in the role models

This PP defines two different roles with the following tasks:

(a) Crypto-officer (authorized to install, configure and maintain the TOE and to create, destruct, backup/restore CSP-SCDs)

(b) Crypto-user (authorized to sign with existing CSP-SCDs)

PKCS#11 on the other hand only defines two roles with the following tasks:

(1) Security Officer (initialize the cryptographic module, define and manage users)

(2) Normal Users (create and delete keys they are using, use cryptographic functions)

As one can see immediately, the two role models don't map directly to each other. Some additional functions are required to allow a mapping between the role model of PKCS#11 and this Protection Profile.

PKCS#11 has been designed to allow several applications to use the cryptographic functions of a (set of) cryptographic token(s) using a single interface. The developers of PKCS#11 had an operational model in mind, where a device is initialized by a security officer (i.e. performing general initialization functions and defining the user(s)) and where the individual users have their "private token objects" that they use to perform cryptographic functions. While this is a suitable model for the use of personal signing devices, the situation within a CA environment is different.

2. Device initialization

The first difference comes up with the initialization of the cryptographic device. Functions additional to PKCS#11 are required to satisfy the operational model underlying this Protection Profile. Any implementation of PKCS#11 will require additional functions, since PKCS#11 deliberately does not specify functions to support aspects like different life cycle phases of a cryptographic token or user management. However, for the PP we need to distinguish between different life-cycle phases of the token. One phase would be the "initialization phase", another one would be the "operational phase".

One possible solution is that in the initialization phase a "System Administrator" (in the words of the PP, "Security Officer" in the words of PKCS#11) would initialize the token and create the first user.

This user ("Crypto Administrator" in the words of the Protection Profile, "Normal User" in the words of PKCS#11) would now be allowed to start "Read/Write" sessions and thus generate a key pair. After creation of the key pair, this Normal User would be reconfigured by the "System Administrator and only allowed to start "Read/Only" sessions, and thus not allowed to create or delete key pairs.

Another possible solution is that the initialization is performed on a separate channel, completely different from PKCS#11. The separate channel could be a different external hardware interface to the HSM, or specialized software running on the same computer over the same hardware interface as PKCS#11. The System Administrator is authenticated over this channel, which also might enforce dual control as required by the Qualified Certificate Policy.

3. Key generation

Solution based on different sessions

As described above, one solution of fulfilling this PP is ensuring that a "normal user" (PKCS#11) who needs to sign data should be allowed to start an R/O session only. In this case a normal user would be equivalent with the Crypto User as defined in this Protection Profile. He is able to perform signature operations but is not able to generate a new key pair, delete a key pair or get access to the private signature key.

In order to create a new key pair, the System Administrator would have to enter a “maintenance mode” and give the “Normal User” the privilege of starting an R/W session, thus changing the Normal User from “Crypto User” into the “Crypto Administrator” in the model of this PP. He than can perform key management functions. When finished, the System Administrator returns the “Normal User” to “Crypto User”.

Solution based on external authentication mechanisms

Another possible solution is to allow the Normal User to start R/W session, but preventing him from creating keys by other means. This could for example be achieved by having the device requesting authentication by a Crypto Administrator (or even N of M administrators) on a different channel every time a key generation request is submitted by the Normal User.

As described above, the separate channel could be a different external hardware interface to the HSM, or specialized software running on the same computer over the same hardware interface as PKCS#11.

In both of these proposed solutions, key generation would thus be performed without ever using the PKCS#11 Security Officer role.

4. Key backup

In PKCS#11 a private token object can be marked as “sensitive” (or “always sensitive”) and “unextractable” (or “never extractable”). In the first case the object can not be exported in unencrypted form, in the second case the object can not be exported at all.

In the view of this Protection Profile a private CA key will be a private token object marked as either “always sensitive” (if key backup is supported) or “ never extractable” (if key backup is not supported).

To support the backup model within the Protection Profile (for tokens that support backup of the private key) functions to extract or restore the encrypted private key (C_WrapKey, C_UnwrapKey) must also either be restricted to the initialization and the maintenance phase, or require additional authentication by a Crypto Administrator over a separate channel as described earlier for key generation.

5. Conclusions

In this annex we have described two examples of a role model compliant with the requirements of the Protection Profile using the PKCS#11 functions. One has to be aware that this is just an outline how to implement the requirements of the PP using PKCS#11. Additional work is required to have full mapping between PKCS#11 and the requirements of this Protection Profile. There may be also other ways to get a PKCS#11 implementation compliant with this PP. The purpose of this section was just to show that the role models of this PP and PKCS#11 can be mapped to each other with some simple extensions to the PKCS#11 interface.