PD CEN/TS 419221-2:2016

BSI Standards Publication

Protection Profiles for TSP cryptographic modules

Part 2: Cryptographic module for CSP signing operations with backup

bsi.

National foreword

This Published Document is the UK implementation of CEN/TS 419221-2:2016.

The UK participation in its preparation was entrusted to Technical Committee IST/17, Cards and personal identification.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

ISBN 978 0 580 92180 3

ICS 35.040; 35.240.30

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 July 2016.

Amendments issued since publication

Date	Text affected

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 419221-2

July 2016

ICS 35.240.30; 35.040

Supersedes CWA 14167-2:2004

English Version

Protection Profiles for TSP cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup

Profils de protection pour modules cryptographiques utilisés par les prestataires de services de confiance - Partie 2 : Module cryptographique utilisé par le prestataire de services de certification pour les opérations de signature avec sauvegarde

Schutzprofile für kryptographische Module von vertrauenswürdigen Dienstanbietern - Teil 2: Schutzprofil für CSP Signieroperationen mit Sicherung

This Technical Specification (CEN/TS) was approved by CEN on 8 May 2016 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

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

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. CEN/TS 419221-2:2016 E

Contents

Page

European foreword

This document (CEN/TS 419221-2:2016) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, the secretariat of which is held by AFNOR.

This document supersedes CWA 14167-2:2004.

This document has been prepared under a mandate given to CEN by the European Commission and the European Free Trade Association.

CEN/TS 419221, *Protection Profiles for TSP cryptographic modules*, is currently composed with the following parts:

— *Part 1: Overview*;

— *Part 2: Cryptographic module for CSP signing operations with backup*;

— *Part 3: Cryptographic module for CSP key generation services*;

— *Part 4: Cryptographic module for CSP signing operations without backup*.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

This 'Cryptographic Module for CSP Signing Operations with Backup - Protection Profile' (CMCSOB-PP) is issued by the European Committee for Standardization.

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 recognized standard for electronic-signature products in the Official Journal of the European Communities.

The document has been prepared as a Protection Profile (PP) following the rules and formats of the Common Criteria version 3.1r3 [CC1] [CC2] [CC3].

The set of algorithms for secure signature-creation devices and parameters for algorithms for secure signature-creation devices is given in a separate document, ETSI/TS 102 176.

This document has been originally prepared as a single Protection Profile and approved as CWA 14167-2:2002. Afterwards, while reviewing this Protection Profile for the evaluation, in order to make it conformant to the Common Criteria 2.1, two Protection Profiles have been created for the same TOE, one including the mandatory function of key backup and the other excluding this function:

— Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP), version 0.28; CWA 14167-2:2004;

— Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP), version 0.28; CWA 14167-4:2004.

Correspondence and comments to this Cryptographic Module for CSP Signing Operations - Protection Profile with Backup (CMCSOB-PP) should be referred to:

Editor: Rémy DAUDIGNY

Email: remy.daudigny@thalesgroup.com

1 Scope

This Technical Specification specifies a protection profile for cryptographic modules used by certification service providers (as specified in Directive 1999/93) for signing operations, with key backup. Target applications include root certification authorities (certification authorities who issue certificates to other CAs and who are at the top of a CA hierarchy) and other certification service providers where there is a high risk of direct physical attacks against the module.

2 Normative references

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

CEN/TS 419221-1:2016, Protection Profiles for TSP cryptographic modules — Part 1: Overview

ETSI/TS 101 456, *Electronic Signature and Infrastructure (ESI); Policy requirements for certification authorities issuing qualified certificates*

ETSI/TS 102 176, *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in CEN/TS 419221-1:2016 apply.

4 PP Introduction

4.1 General

This clause provides document management and overview information that is required to carry out protection profile registry. Therefore, Subclause 4.2 “PP Reference” gives labelling and descriptive information necessary for registering the Protection Profile (PP). Subclause 4.3 “Protection Profile Overview” summarizes the PP in narrative form. Subclause 4.4 “TOE Overview” summarizes the TOE in a narrative form. As such, these subclauses give an overview to the potential user to decide whether the PP is of interest. It is usable as standalone abstract in PP catalogues and registers.

4.2 PP Reference

Title	Cryptographic Module for CSP Signing Operations with backup – Protection Profile
CC revision	v3.1 release 3
PP version	v0.35
Authors	Rémy Daudigny
Publication Date	2015
Keywords	cryptographic module, CSP signing device, qualified certificate signing, certificate status information signing
Registration	419221–2

4.3 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), 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.*

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 key pairs, and their usage for the creation and verification of advanced electronic signatures in qualified certificates or certificate status information. The private keys are referred to in this PP as Certification Service Provider Signature-Creation Data (CSP-SCD). The public keys are referred as Certification Service Provider Signature-Verification Data (CSP-SVD).

The Protection Profile's primary scope is for signing qualified certificates. However 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. It may also be used for other trusted service providers creating electronic signatures.

This PP is Common Criteria Part 2 extended and Common Criteria Part 3 conformant. The assurance level for this PP is EAL4, augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis).

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 recognized 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.

1) In the remainder of this PP the term 'Certificate Service Provider (CSP)' is used instead of the commonly used term 'Certification Authority (CA)', as the former is employed by the Directive EC 1999/93 [1] this PP aims to support.

4.4 TOE Overview

4.4.1 TOE type

The TOE is a Cryptographic Module (CM) used for the creation and usage of Certificate Service Provider 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:

a) generation of CSP-SCD;

b) usage of the CSP-SCD to create advanced electronic signatures for qualified certificates based on either:

   1) the hash value of the content of the qualified certificate, or

   2) an intermediate hash-value of a first part of the qualified certificate and a remaining part of the qualified certificate or

   3) the complete content of the qualified certificate, where the hashing is also performed in the CM (optional).

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 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:

c) CSP Signature Creation Data (CSP-SCD): private key of CSP, created and stored internally in the TOE;

d) data to be signed representation (DTBS-representation): the data to be signed by the TOE may e.g. be:

   1) Certificate hash value: imported to the TOE;

   2) Certificate contents (optional, when hashing is performed in the TOE), data to be hashed (fully or partially) and signed, imported to the TOE;

   3) other data to be signed by the TOE, such as CRL or the hash value of the CRL, or time-stamping content data;

e) certificate signature: created signature, exported from the TOE.

The TOE supports backup and restoration of CSP-SCD, other user data and TSF data to re-establish 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 while the IT-environment will ensure the availability of the backup data.

For the cryptographic functions, the TOE shall support the cryptographic algorithms specified in ETSI/TS 102 176, or a subset thereof.

4.4.2 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 data of keys);
- **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 of TOE users shall be identity-based.

Maintenance of the TOE as well as the management of the CSP-SCDs are 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 Auditor and Security officer of the CSP [CEN] the individual users shall be known by the TOE as Auditor and Crypto-officer and the TOE needs to perform identity 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.

The TOE manages two or more user identities for the role Crypto-officer to allow dual person control for security critical actions like generation of CSP-SCD and CSP-SVD generation, backup and restore. The end-users may access to the TOE signing service through a client application in the TOE environment. The client application acts as agent for these end-users with a TOE user identity in the Crypto-user role.

4.4.3 Usage and major security features of the TOE

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 in the IT environment. 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.

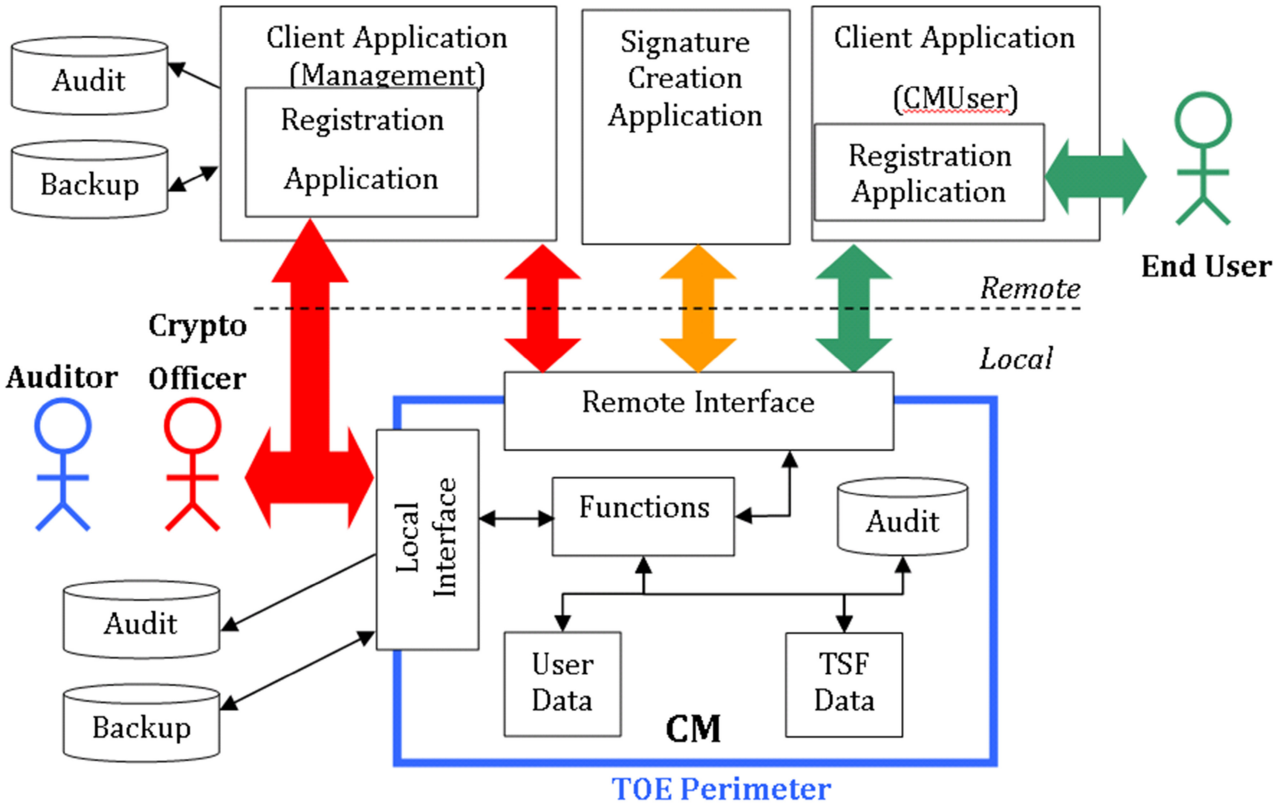


Figure 1 — TOE general overview

NOTE This diagram is illustrative. It needs not represent the exact implementation architecture.

As shown in Figure 1, no relation exists with Trusted Service Providers (TSP). The end-users will communicate with the client application, which in turn will call TOE services on behalf of the end-user. The client application provides the human interface for user identification and authentication. 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.

The TOE provides identification authentication, access control and audit for users of its services. The client application in the TOE environment may mediate the TOE signing function to its end-users. Therefore it is the responsibility of the client application to identify, authenticate and control access of its end-users gaining access to the TOE services provided for the Crypto-user role. The end-users authenticate themselves to the client application with his or her identity. The client application checks the authorization of the end-user for the TOE signing service. If the end-user is allowed to use the signing function the client application will authenticate them for the Crypto-user role to the TOE and will map the identity of the end-user to the Crypto-user role.

The client application performs 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:

a) a registration application, which initializes the information for the certificate;

b) a signature-creation application, which may be:

1) 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

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

When exporting the CSP-SCD or TSF data the TOE ensures the confidentiality and integrity of the CSP-SCD and the TSF data by the backup and restoration functions. The backup will export user data and TSF data (backup data) and the restore function will import the backup data for recreation of the state of the TOE at the time the backup was created. The IT-environment provides means of supporting the backup and restore functions of the TOE by ensuring the availability of the backup data.

Privileged users as Crypto-officer and Auditor can interact with the TOE through the local interface. They can also connect remotely to the TOE thanks to a Client Application that offers Management capabilities. This application performs identity-based auditing to support accountability for the privileged operations. The Client Application used for Management purposes and the Client Application used by the end-user are represented in Figure 1 as separate applications. Nevertheless, they are very similar (RBAC authentication, Registration of user for accountability…) and rely on the same security functions for protecting communications with the Cryptomodule.

Finally, the TOE supports a secure firmware update mechanism where updating data are protected in integrity, confidentiality and authenticity (signed).

4.4.4 Available non-TOE hardware/software/firmware

None. The TOE is an independent Cryptographic Module comprising its own hardware and software.

5 Conformance Claim

5.1 CC Conformance Claim

This protection profile is conformant to Common Criteria version 3.1 revision 3.

More precisely, this protection profile is:

— CC Part 1 [CC1],

— CC Part 2 extended [CC2],

— CC Part 3 conformant [CC3].

The assurance requirement of this Protection Profile is **EAL4 augmented**.

Augmentation results from the selection of:

— AVA_VAN.5 Advanced methodical vulnerability analysis

5.2 PP Claim

This PP does not claim conformance to any another Protection Profile.

5.3 Conformance Rationale

Since this PP is not claiming conformance to any other protection profile, no rationale is necessary here.

5.4 Conformance Statement

This PP requires strict conformance of any ST or PP, which claims conformance to this PP.

6 Security Problem Definition

6.1 Assets

6.1.1 General

The primary assets that need to be protected by the TOE are presented below.

6.1.2 TOE services

R.SERVICES (I, A)

TOE services are:

1) generation and management (usage and destruction) of CSP key pair (SCD and SVD)

2) usage of CSP-SCD for signature

3) backup and restoration of TSF data

4) User Identity and Role management

5) Internal Audit

These services shall be protected in Integrity and Availability.

6.1.3 TOE Data

6.1.3.1 Keys

R.CSP-SCD (C, I, A)

As defined in the Directive ([1] Article 2 Paragraph 4) a Certification Service Provider Signature Creation Data (R.CSP-SCD) means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

CSP-SCD is a cryptographic private key that shall be protected in Confidentiality, Integrity and Availability.

R.CSP-SVD (I)

As defined in the Directive ([1] Article 2 Paragraph 4) a Certification Service Provider Signature Verification Data (R.CSP-SVD) means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;

The CSP-SVD shall be protected in Integrity.

R.BACKUP_KEY (C, I)

A cryptographic key used to provide a cryptographic checksum of backup data and encrypt backup data before exporting it to the TOE environment.

The cryptographic checksum for R.BACKUP_DATA shall be based on symmetric cryptographic algorithms (e.g. keyed hash) or asymmetric cryptographic algorithms (e.g. digital signatures).

R.BACKUP_KEY shall be protected in confidentiality and integrity.

R.BACKUP_KEY is kept by the TOE environment.

Application note: R.BACKUP_KEY may be a dual asset, depending on the developer implementation choices, divided in a cryptographic key to ensure integrity of R.BACKUP through the checksum and a cryptographic key to encrypt it.

6.1.3.2 Internal TOE Data

R.CM_FIRMWARE (I, Auth)

Embedded firmware of the cryptomodule.

The firmware implements the security mechanisms of the TOE, therefore it needs to be protected in integrity inside the cryptomodule.

Moreover, as far as a firmware update process might be available during operational lifecycle steps of the TOE, updating data authenticity shall be checked by the cryptomodule prior to the installation.

This asset shall be protected in integrity and authenticity.

R.TSF_DATA (C, I, A)

TSF data includes:

— VAD and RAD;

— other system data not related to a user or role (system configuration data, audit data).

TSF data shall be protected in confidentiality, integrity and availability.

R.USERMGMT_DATA (I)

Non-confidential data related to a user or role (identifier, access control lists, role definitions, etc.).

This asset shall be protected in integrity.

6.1.3.3 External TOE Data

R.BACKUP_DATA (C, I)

Backup data are R.TSF_DATA and R.CSP-SCD, encrypted by R.BACKUP_KEY, with a cryptographic checksum, exported from the TOE, by the TOE, to the TOE environment and restored into the TOE.

This asset needs to be protected in confidentiality and integrity.

Availability of this data shall be ensured in the TOE environment.

R.DTBS_Representation (I)

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, i.e. the complete electronic data to be signed, such as QC content data or certificate status information.

The client indicates to the TOE the case of R.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.

R.DTBS_Representation shall be protected in integrity.

R.DSD (Auth)

Digitally Signed Data (DSD) is the result of the TOE signature function over the R.DTBS_Representation.

For example, R.DSD can be a time-stamp, a certificate, a certificate revocation list, a certificate status information, an online certificate status protocol (OCSP) messages or a CSP digital signature.

R.DSD shall be protected in authenticity.

6.2 Threats

6.2.1 General

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

6.2.2 Threat agents

TA.EXTERNAL

This agent represents an entity that does not hold any authorized role to operate or interact with the TOE. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE.

Examples of this threat agent are:

— unauthorized CSP personnel,

— cybercriminals,

— hackers in general.

TA.INSIDER

This agent represents an entity that holds an authorized role to operate or interact with the TOE, and which has the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE.

Examples of this threat agent are:

— auditors,

— crypto-officers.

TA.INADVERTENT

This agent represents an entity that holds an authorized role to operate or interact with the TOE, but which does not have the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces, or even have direct physical access to the TOE.

Examples of this threat agent are:

— crypto-users via the cryptomodule-user role

— auditors,

— crypto-officers.

6.2.3 Threats description

6.2.3.1 Threats on Keys

T.BACKUP_KEY_Alteration *Alteration of backup key*

TA.EXTERNAL or TA.INSIDER might modify or alter R.BACKUP_KEY by interaction with the TOE logical internal functions, or within the TOE environment, in order to:

— invalidate the cryptographic checksum of R.BACKUP_DATA or

— invalidate decryption of R.BACKUP_DATA.

TA.INADVERTENT might also modify or alter R.BACKUP_KEY in the TOE environment within the session of a Crypto-officer whose responsibility is to load this data in the cryptomodule.

T.BACKUP_KEY_Derive Derivation of R.BACKUP_KEY

TA.EXTERNAL or TA.INSIDER might derive all or part of R.BACKUP_KEY using knowledge about the R.BACKUP_KEY operations (generation, usage, destruction), even during legitimate use of R.SERVICES.

T.BACKUP_KEY_Disclose *Disclosure of R.BACKUP_KEY*

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

T.CSP-SCD_Alteration *Alteration of the R.CSP-SCD*

TA.EXTERNAL or TA.INSIDER might modify or alter R.CSP-SCD by interaction with the TOE logical internal functions, in order to invalidate the electronic signature of R.DTBS_Representation.

Although the use of a distorted CSP-SCD can be detected, the impacts for the organization issuing the signed data using the CSP-SCD (e.g. qualified certificates) can be high.

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

TA.EXTERNAL or TA.INSIDER might derive all or part of R.CSP-SCD using knowledge about the R.CSP-SCD operations (generation, usage and destruction), R.DTBS or R.CSP-SVD, even during legitimate use of R.SERVICES.

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

TA.EXTERNAL or TA.INSIDER might disclose all or part of R.CSP-SCD over physical or logical TOE interface by bypassing the export control mechanisms.

T.CSP-SVD_Alteration *Alteration of the R.CSP-SVD*

TA.EXTERNAL or TA.INSIDER might alter R.CSP-SVD when R.CSP-SVD is exported from the TOE.

Although the use of a distorted CSP-SVD can be detected, the impacts for the organization issuing the signed data using the CSP-SCD (e.g. qualified certificates) can be high.

6.2.3.2 Threats on internal TOE Data

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

TA.EXTERNAL or TA.INSIDER might try to modify or alter R.CM_FIRMWARE by loading malicious software into the TOE or interacting with the TOE logical interfaces, in order to modify or gain access to R.CSP-SCD, R.TSF_DATA, R.USERMGMT_DATA, R.BACKUP_KEY or R.SERVICES.

6.2.3.3 Threats on external TOE Data

T.Backup *Forging or corrupting backup data*

TA.EXTERNAL, TA.INSIDER or TA.INADVERTENT might corrupt R.BACKUP_DATA within the TOE environment.

For instance, TA.INSIDER such as CSP personnel without expected clearance may forge backup data (R.BACKUP_DATA) for restoring forged VAD and RAD (R.TSF_DATA) into the TOE, in order to gain illicit access to R.SERVICES.

Finally, this threat might also lead for example to corruption of R.BACKUP_DATA within the TOE environment by TA.INADVERTENT, and R.TSF_DATA might be lost.

T.Data_Manipul *Manipulating data outside of the TOE*

TA.EXTERNAL or TA.INSIDER might manipulate R.DTBS_Representation within the TOE environment during its transfer from the client application to the TOE. This may result in the effect that the TOE signs data (corrupted R.DTBS_Representation) without the approval of the user under whose control the data are 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 might also occurs on R.USERMGMT_DATA within the session of a Crypto-officer whose responsibility is to load this data in the cryptomodule.

6.2.3.4 Threats on TOE Services

T.Insecure_Init *Insecure initialization of the TOE*

TA.INSIDER or TA.INADVERTENT may initialize the TOE with insecure R.TSF_DATA, R.USERMGMT_DATA.

For example, TA.INADVERTENT may initialize the TOE (R.SERVICES_4) with an outdated access control list (R.USERMANGT_DATA).

T.Malfunction *Malfunction of TOE*

There is no active agent for this threat.

An internal malfunction of TOE functions may result in:

- the modification of R.DTBS_Representation,
- misuse of R.SERVICES,
- disclosure or alteration of R.CSP-SCD
- disclosure or alteration of R.BACKUP_KEY
- denial of R.SERVICES for authorized users
- alteration of R.TSF_DATA or R.USERMGMT_DATA

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

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

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

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

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

- the central processing unit
- a coprocessor for accelerating cryptographic operations
- a physical random number generator
- storage devices used to store the R.CSP-SCD or the DTBS-representation
- physical I/O device drivers

T.Phys_Manipul *Physical Manipulation of the TOE*

TA.EXTERNAL or TA.INSIDER may try to physically manipulate the TOE with the intent to:

- derive, disclose or alter R.CSP-SCD (by side channel for example) or,
- derive, disclose or alter R.BACKUP_KEY
- manipulate the R.DTBS_Representation within the TOE
- misuse R.SERVICES
- alter R.TSF_DATA

The TOE may be physically attacked by even an authorized user of TOE services.

This threat includes also the destruction of the TOE by deliberate action.

T.KeyGeneration_Misuse *Misuse of the keys generation function*

TA.EXTERNAL, TA.INSIDER or TA.INADVERTENT may misuse R.SERVICES to produce unauthorized R.CSP-SCD and R.CSP-SVD.

For instance TA.INSIDER such as CSP personnel without expected clearance may misuse the generation of CSP key pair function (R.SERVICES_1) resulting in producing certificates (R.DSD) signed by an unauthorized R.CSP-SCD.

T. Signature_Misuse *Misuse of signature-creation function*

TA.EXTERNAL or TA.INSIDER misuses R.SERVICES for signature-creation to produce unauthorized R.DSD.

For instance, TA.EXTERNAL or TA.INSIDER may bypass the user identity management function (R.SERVICES_4) for signing unauthorized certificates (R.DSD) with the R.CSP-SCD (R.SERVICES_2).

T.Signature_Forgery *Forgery of digital signature*

TA.EXTERNAL or TA.INSIDER exploits weaknesses in R.SERVICES in order to forge R.DSD in a way that is not detectable by the verifier of the signature.

For instance, TA.INSIDER exploits weaknesses into the cryptography and/or key management (resp. R.SERVICES_2 and/or R.SERVICES_1) in order to forge a certificate (R.DSD).

6.2.4 Threats vs Threat agents

Assets	Threats	TA.EXTERNAL	TA.INSIDER	TA.INADVERTENT
Keys	**T.BACKUP_KEY_Alteration**	X	X	X

	T.BACKUP_KEY_Derive	X	X	
	T.BACKUP_KEY_Disclose	X	X	
	T.CSP-SCD_Alteration	X	X	
	T.CSP-SCD_Derive	X	X	
	T.CSP-SCD_Disclose	X	X	
	T.CSP-SVD_Alteration	X	X	
Internal Data	**T.Bad_SW**	X	X	
External Data	**T.Backup**	X	X	X
	T.Data_Manipul	X	X	
Services	**T.Insecure_Init**		X	X
	T.Malfunction	*No Active Threat Agent*		
	T.Phys_Manipul	X	X	
	T.KeyGeneration_Misuse	X	X	X
	T.Signature_Misuse	X	X	
	T.Signature_Forgery	X	X	

6.3 Organizational Security Policies

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

Only algorithms and algorithm parameters (e.g. key length) approved for being used for signature creation by trustworthy systems shall be used to e.g. generate qualified certificates or to sign certificate status information.

The TOE shall support cryptographic algorithm and key length conformant to the rules defined by the relevant CC Certification Body.

> The ST writer should consult the notified body or the certification body for the admissible algorithms, cryptographic key sizes and other parameters for algorithms, and standards for digital signature-creation by SSCD

A list of recommended algorithms and parameters is given in ETSI/TS 102 176. Where confidentiality or integrity protection services are required, such as for example for backup of R.CSP-SCD, only cryptographic strong algorithms and algorithm parameters shall be used.

6.4 Assumptions

A.Audit_Support *CSP audit review*

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

A.Secure_Channel *Interface with Human Users*

The client application and the management application (see Figure 1) 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.CryptoUser_Agent *Authentication of Users*

The client-application is assumed as user of the TOE in the Crypto-user role. Other users authorized 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.

A.Trusted_Environment Trustworthiness of operating personnel and physical security

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

A.Data_Store *Storage and Handling of TOE data*

The TOE environment ensures the confidentiality, integrity and availability of their security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE. The TOE environment ensures the availability of the encrypted backup data. Examples of these data are verification authentication data, cryptographic key material and documentation of TOE configuration data.

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 initialized 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.

7 Security Objectives

7.1 General

This clause identifies and defines the security objectives for the TOE and its operational environment.

Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organizational security policies and assumptions.

7.2 Security Objectives for the TOE

O.Audit *Generation and Export of Audit Data*

The TOE shall audit the following events:

- TOE initialization;
- TOE start-up;
- generation of R.CSP-SCD;

- destruction of R.CSP-SCD;
- unsuccessful authentication (R.TSF_DATA);
- modification of TOE management data (R.MNGT_DATA);
- addition of new users or roles (R.MNGT_DATA);
- deletion of users or roles (R.MNGT_DATA);
- reading and deleting audit trail records;
- generation, export, import and destruction of backup data (R.BACKUP_DATA);
- restoration of backup data (R.BACKUP_DATA);
- unsuccessful restoration attempt of backup data (R.BACKUP_DATA);
- generation, export, import and destruction of backup key (R.BACKUP_KEY);
- firmware (R.CM_FIRMWARE) modification (R.TSF_DATA);
- execution of the TSF self-tests during initial start-up, at the request of the authorized user, during installation and maintenance (R.TSF_DATA);
- unsuccessful self-test operations (R.TSF_DATA);
- tamper detection event (R.TSF_DATA).

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

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

The confidentiality and integrity of the R.CSP-SCD shall be ensured during their whole lifetime.

The TOE shall ensure cryptographic secure R.CSP-SCD generation, use and management. This includes protection against disclosing completely or partly the R.CSP-SCD through any physical or logical TOE interface.

O.BACKUP_KEY_Secure *Secure R.BACKUP_KEY Generation and Management*

The confidentiality and integrity of the R.BACKUP_KEY shall be ensured during their whole lifetime.

The TOE shall ensure cryptographic secure R.BACKUP_KEY generation, use and management. This includes protection against disclosing completely or partly the R.BACKUP_KEY 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. This includes integrity checks and/or authenticity of TOE software, firmware, internal TSF data or user data during initial start-up, at the request of the authorized user, randomly during the critical steps of cryptographic process, during installation and maintenance.

O.RBAC *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 initialization phase.

O.Attack_Response *Response to Physical Attacks*

The TOE shall detect attempts of physical tampering and securely destroy the R.CSP-SCD and R.BACKUP_KEY.

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

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

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

The TOE shall not export data except for R.BACKUP_DATA and R.CSP-SVD.

The TOE shall apply integrity and confidentiality protection measures when exporting R_BACKUP_DATA for backup purposes.

Backup and restore operations shall be audited and the audit data shall associate these events with the identity of the users.

The TOE shall apply integrity protection measures when exporting R.CSP-SVD.

O.Sign_Secure *Secure advanced signature-creation*

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

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

O.Backup_Secure

The TOE creates cryptographic checksum and encrypts backup data (R.BACKUP_DATA) that

- do not reveal R.BACKUP_KEY and
- cannot be forged without knowledge of the R.BACKUP_KEY
- cannot be decrypted without knowledge of the R.BACKUP_KEY.

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 userbased.

7.3 Security Objectives for the Operational 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

OE.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 cannot be performed within the TOE.

Security controls in the TOE environment shall also prevent unauthorized manipulation of data once submitted to the TOE.

OE.Audit *Audit review*

The environment ensures the availability of the generated and exported by the TOE audit trails and provides a review of the audit trail recorded by the TOE.

OE.Secure_Channel *Reliable Human Interface*

The client application provides a human interface and the means to establish a secure communication path between human users and the TOE. Confidentiality and integrity of the data transferred between the TOE and the human user are ensured by the secure communication path.

OE.Personnel *Reliable Personnel*

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

OE.Protect_Access *Prevention of Unauthorized Physical Access*

The TOE shall be protected by physical, logical and organizational protection measures, in order to prevent any TOE modification, as well as any protected assets disclosure. Those measures shall restrict the TOE usage to authorized persons only. This objective shall follow the policies requirements from ETSI/TS 101 456.

OE.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 (i.e. if TOE is blocked in its secure state after a failure, service discontinuity or detected physical tampering). 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.

OE.Secure_Init *Secure Initialization Procedures*

Procedures and controls in the TOE environment shall be defined and applied that allow to securely set-up and initialize the TOE for the generation of signatures for qualified certificates or certificate status information. This includes the secure key generation / key import, encryption and cryptographic checksum capabilities of the TOE, as well as the initial configuration of other TSF data like roles, users and user authentication information.

OE.Secure_Oper *Secure Operating Procedures*

Procedures and controls in the TOE environment shall be defined that allow operating the TOE within a CA system.

NOTE The CA system will comply with the requirements of the EU Directive and the Policy for certification authorities issuing qualified certificates.

8 Extended Components Definitions

8.1 Extended Component Definitions

8.1.1 Family FCS_RND

The TOE shall generate R.CSP-SCD with high cryptographic quality using random number generators.

The new component FCS_RND aim at specifying metrics over random number generator used in the cryptographic operations described in FCS_COP.

FCS_RND.1 requires the ST editor to define the quality metric of the random numbers used by the TOE to generate the R.CSP-SCD.

In CC part 2, FIA_SOS.2 seems similar to FCS_RND.1 but FIA_SOS.2 is limited to generation of secrets used only as authentication information.

FCS_RND generation of random numbers

Family behaviour

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

Component levelling

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

Management: FCS_RND.1

There are no management activities foreseen.

Audit: FCS_RND.1

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

a) Minimal: Failure of the random number generator.

FCS_RND.1 Quality metrics for random numbers

Hierarchical to: no other components.

FCS_RND.1.1

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

FCS_RND.1.2

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

Dependencies:

FPT_TST.1 TSF testing. FCS_COP.1 Cryptographic operation

8.1.2 Family FDP_BKP

The cryptographic module (CM) supports backup of R.CSP-SCD, other user data and TSF data to restore the operational state of the same CM or for a new CM 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 CM 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 new component belongs to FDP because it concerns export of data from the TOE. However, it is necessary to specify a new component FDP_BKP to introduce and specify the precise operations performed by the backup and restore operations.

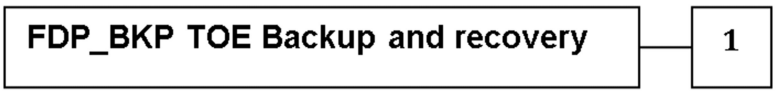
The specific requirements address the protection of R.CSP-SCD, other cryptographic keys and TSF data for backup and recovery.

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 be capable of invoking the backup function on demand.

FDP_BKP.1.2

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 (R.BACKUP_DATA);

2) a stored copy of the backup data (R.BACKUP_DATA);

3) the cryptographic key(s) (R.BACKUP_KEY) needed to decrypt the R.CSP-SCD and any other encrypted critical security parameters;

4) the cryptographic key(s) needed to verify the cryptographic checksum of the backup data (R.BACKUP_KEY).

FDP_BKP.1.3

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

FDP_BKP.1.4

The R.CSP-SCD, other critical security parameters and other confidential information shall be exported in encrypted form only.

FDP_BKP.1.5

The backup data (R.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

9 Security Requirements

9.1 General

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

Security functional requirements components given in 9.3 “Security Functional Requirements” are drawn from Common Criteria part 2 [CC2]. Some security functional requirements represent extensions to [CC2], with a reasoning given in 9.5. 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 9.4 “Security Assurance Requirement” are drawn from the security assurance components from Common Criteria part 3 [CC3].

9.2 Subjects, objects, security attributes and operations

9.2.1 General

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

9.2.2 Subjects

a) Subjects are the users of the TOE.

b) A User holds an authorized role to access the services available in the TOE.

c) Defined Roles for the TOE are:

   1) crypto-user,

   2) crypto-officer,

   3) auditor.

9.2.3 TOE Objects and security attributes

— Certification Service Provider – 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.

— Certification Service Provider – 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 or the certificate status information.

— Audit data: means a set of data that reflects operations performed on the TOE regarding its internal security

— Backup Data: means CSP-SCD, the TSF data and the system data sufficient to recreate the state of the TOE at the time the backup was created.

— User's identity. Set of data that uniquely describes and identifies a user of the TOE.

— Role. Set of permissions granted to a user of the TOE to perform certain operations on the TOE.

— TSF data related to users and roles. Information about the TOE Security Functionality (TSF), but restricted to users and roles. This includes users' RAD, identifier and assigned roles, the access control lists and role definitions, as well as any other information used by the TOE to authenticate users and grant accesses.

9.2.4 TOE Operations

— Generate CSP SCD/SVD pair in order, for example, to produce Certificate, an electronic attestation which links the SVD to a person and confirms the identity of that person

— Digitally Sign 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

— Backup means export of the backup data. Note that backup is the only function which is allowed to export CSP-SCD and only if backup package is implemented

— Export (transmit) audit data. Operation by which a user of the TOE uses the TOE to export audit data from the TOE to the TOE environment.

— Delete audit data. Operation by which a user of the TOE uses the TOE to delete audit data.

— Query one's own RAD, users' identity, roles and binding between users and roles. Operation by which a user of the TOE uses the TOE to access to certain information related to the users, including its own RAD, the identity of users of the TOE, the existing roles, and the roles assigned to the users of the TOE.

— Modify one's own RAD, users' identity, roles and binding between users and roles. Operation by which a user of the TOE uses the TOE to access to and modify certain information related to the users, including its own RAD, the identity of users of the TOE, the existing roles, and the roles assigned to the users of the TOE.

— Delete users' identity, roles and binding between users and roles. Operation by which a user of the TOE uses the TOE to delete certain information related to the users, including its own RAD, the identity of users of the TOE, the existing roles, and the roles assigned to the users of the TOE.

9.3 Security Functional Requirements

9.3.1 General

Note that the national laws for electronic signatures may require disabling any backup function of the R.CSP-SCD if the CM is used by CSP under the national regulation. If enabling and disabling of the backup and restore functions shall be supported by the TOE the ST writer will include appropriate security functional requirements by means of the components FMT_MOF.1 and FMT_SMF.1.

According to CC part 1 the refinements provided in this subclause are operations of the security functional requirements and therefore are mandatory parts. The application notes are optional part of the PP and contain additional supporting information that is considered relevant or useful for the construction, evaluation, or use of the TOE but they are not mandatory to fit.

9.3.2 Security audit (FAU)

9.3.2.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1

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

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

b) All auditable events for the not specified level of audit; and

c) • Initialization of the TOE, Start-up after power up,

• Shutdown of the TOE,

• Cryptographic key generation (FCS_CKM.1): R.CSP-SCD/R.CSP-SVD pair generation, R.BACKUP_KEY generation

• Cryptographic key distribution (FCS_CKM.2): entry of R.BACKUP_KEY

• Cryptographic key destruction (FCS_CKM.4): R.CSP-SCD destruction, destruction of R.BACKUP_KEY

• Failure of the random number generator (FCS_RND.1)

• 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 (R.BACKUP_DATA)

• 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 initialization (FMT_MSA.3): modifications of the default setting of permissive or restrictive rules, all modifications of the initial values of security attributes;

• Management of TSF data (FMT_MTD.1/ACCESS_CONTROL): All modifications to the values of TSF data,

• Management of TSF data (FMT_MTD.1/AUDIT: Export of audit data, Clear of audit data,

• Failure with preservation of secure state (FPT_FLS.1): Failure detection of the TSF and secure state,

• Inter-TSF detection of modification (FPT_ITI.1): The detection of modification of imported backed up TSF data

• Notification of physical attack (FPT_PHP.2): Detection of intrusion,

• TSF testing (FPT_TST.1): Execution of the TSF self-tests during initial start-up, at the request of the authorized user, during installation and maintenance and the results of the tests, unsuccessful self-test operations.

FAU_GEN.1.2

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, identity of the user and sequence data.

Refined by adding:

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

Application note:

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).

9.3.2.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1

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

9.3.2.3 Guarantees of audit data availability (FAU_STG.2)

FAU_STG.2.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2

The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3

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

Application note:

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

1) stop the normal operation,

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

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

9.3.3 Cryptographic support (FCS)

9.3.3.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

9.3.3.2 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1

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

All secret or private keys entered into the TOE shall be protected in confidentiality and respect the organizational Security Policy ***P.Algorithms***.

Key entry shall be performed using either manual or electronic methods.

Secret and private keys established using manual methods shall be entered either:

1) in encrypted form or

2) using split knowledge procedures.

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.

If split knowledge procedures are used:

3) The TOE shall separately authenticate the crypto-officer entering each key component.

4) At least two key components shall be required to reconstruct the original cryptographic key.

Application note:

Due to FPT_FLS.1 and FPT_PHP.3 with their refinements the TOE would not store permanently any private or secret key because this key will be erased after detection of failure or physical tampering. The TSF shall import all secret backup key(s) to restore the TOE to an operational status at a previous point in time. The import of encrypted keys requires a clear key to decrypt these keys in the TOE. Therefore FCS_CKM.2 ensures that the master key under which all other keys are encrypted for import

into the TOE shall be imported by split knowledge procedures. Note that according to FDP_BKP.1.4 the R.CSP-SCD shall be exported for backup and imported for restore in encrypted form only.

9.3.3.3 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 R.CSP-SCD and all other plaintext secret or private keys, if the TSF required by FPT_PHP.2 detects physical tampering.

9.3.3.4 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: [assignment: *list of standards*].

Refined by adding:

The standards for digital signature-creation shall respect the organizational Security Policy ***P.Algorithms***.

9.3.3.5 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: [assignment: *list of standards*].

Refined by adding:

The standards for encryption and decryption shall respect ***P.Algorithms***

9.3.3.6 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: [assignment: *list of standards*].

Refined by adding:

The standards for calculation and verification of cryptographic checksums shall respect ***P.Algorithms***

9.3.3.7 Quality metrics for random numbers (FCS_RND.1)

FCS_RND.1.1

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

FCS_RND.1.2

The TSF shall be able to enforce the use of TSF-generated random numbers for FCS_CKM.1.

Application Note:

The chosen quality metric algorithm shall respect ***P.Algorithms***.

9.3.4 User data protection (FDP)

9.3.4.1 Subset access control (FDP_ACC.1/CRYPTO)

FDP_ACC.1.1/CRYPTO

The TSF shall enforce the Crypto-SFP on

- User,
- R.CSP-SCD,
- R.CSP-SVD,
- R.BACKUP_KEY
- DTBS representation,
- generated R.CSP-SCD/R.CSP-SVD pair (FCS_CKM.1),
- destruction of R.CSP-SCD, R.CSP-SVD, R.BACKUP_KEY (FCS_CKM.4),
- signed DTBS representation (FCS_COP.1/SIGN).

9.3.4.2 Subset access control (FDP_ACC.1/AUDIT)

FDP_ACC.1.1/AUDIT

The TSF shall enforce the Audit-SFP on:

- User;
- Audit data;
- export operations
- delete operations.

9.3.4.3 Subset access control (FDP_ACC.1/BACKUP)

FDP_ACC.1.1/BACKUP

The TSF shall enforce the Backup SFP on

- User;
- R.CSP-SCD,
- R.BACKUP_KEY,
- R.BACKUP_DATA,
- backup (FDP_BKP.1),
- restore (FDP_BKP.1),

- R.BACKUP_KEY entry (FCS_CKM.2).

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

FDP_ACF.1.1/ CRYPTO

The TSF shall enforce the Crypto-SFP to objects based on the following: 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 R.CSP-SCD, R.CSP-SVD and R.BACKUP_KEY under, at least, dual person control.

2) User with security attribute Role Crypto-officer is allowed to destruct (FCS_CKM.4) the objects R.CSP-SCD, R.CSP-SVD and R.BACKUP_KEY.

3) User with security attribute Role Crypto-officer is allowed to export R.CSP-SVD.

4) User with security attribute Role Crypto-officer is allowed to export R.BACKUP_KEY.

5) User with security attribute Role Crypto-user is allowed to create signature of the DTBS-representation with R.CSP-SCD (FCS_COP.1/SIGN).

6) User with security attribute Role Crypto-user is allowed to export R.CSP-SVD.

FDP_ACF.1.3/CRYPTO

The TSF shall explicitly authorize 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 additional rules: User with security attribute Role Crypto-user is not allowed

a) to generate (FCS_CKM.1) the objects R.CSP-SCD, R.CSP-SVD and R.BACKUP_KEY,

b) to destruct (FCS_CKM.4) the objects R.CSP-SCD, R.CSP-SVD and R.BACKUP_KEY.

Application note:

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

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

FDP_ACF.1.1/AUDIT

The TSF shall enforce the Audit-SFP to objects based on the following: 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:

a) Users with security attribute Role Auditor are allowed:

   1) to export Audit data,

2) to clear Audit data.

b) Users with security attribute Role Crypto-officer are allowed to export Audit data.

FDP_ACF.1.3/AUDIT

The TSF shall explicitly authorize 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 additional rules:

1) Users with security attribute Role Crypto-officer are not allowed to delete Audit data

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

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

FDP_ACF.1.1/BACKUP

The TSF shall enforce the Backup SFP to objects based on the following: 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, at least, dual person control

a) to backup R.CSP-SCD and R.CSP-SVD (FDP_BKP.1),

b) to restore R.CSP-SCD and R.CSP-SVD (FDP_BKP.1),

c) to enter R.BACKUP_KEY (FCS_CKM.2).

Application note:

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

FDP_ACF.1.3/BACKUP

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes that explicitly authorize access of subjects to objects*].

FDP_ACF.1.4/BACKUP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: User with security attribute Role Crypto-user is not allowed:

d) to backup R.CSP-SCD (FDP_BKP.1),

e) to restore R.CSP-SCD (FDP_BKP.1),

f) to enter a backup key (FCS_CKM.2).

Application note:

If the TSF implementing FDP_BKP.1 does not support separate backup for R.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.

9.3.4.7 Backup and recovery (FDP_BKP.1)

FDP_BKP.1.1

The TSF shall be capable of invoking the backup function on demand.

FDP_BKP.1.2

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 R.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.1.3

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

FDP_BKP.1.4

The R.CSP-SCD, other critical security parameters and other confidential information shall be exported in encrypted form only.

FDP_BKP.1.5

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

9.3.4.8 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 TOE.

FDP_ETC.1.2

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

9.3.4.9 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: R.CSP-SCD, R.BACKUP_KEY and R.TSF_DATA (RAD).

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

FDP_SDI.2.1

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

FDP_SDI.2.2

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

Refined by adding:

The TSF are not required to monitor the DTBS representation for integrity errors.

Application note:

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

The secure state is defined in FPT_FLS.1 (see 9.3.8.1)

9.3.5 Identification and authentication (FIA)

9.3.5.1 General

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 signing of DTBS by the cryptographic module.

9.3.5.2 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1

The TSF shall detect when *[selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]]* 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 level of threat (high attack potential). If all identities are blocked by FIA_AFL.1 then the TOE is not operational.

9.3.5.3 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.

9.3.5.4 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 level of threat (high attack potential) and applies to authentication mechanism to be implemented in the TOE.

9.3.5.5 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 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.

9.3.5.6 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.

9.3.6 Security management (FMT)

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

FMT_MSA.1.1/ROLE_CRYPTO

The TSF shall enforce the Backup SFP and Crypto-SFP to restrict the ability to query, modify and delete [assignment: *other operations*] the security attributes Role Crypto-user and Role Crypto-officer to Crypto-officer.

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

FMT_MSA.1.1/ROLE_AUDIT

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

9.3.6.3 Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1

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

9.3.6.4 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1

The TSF shall enforce the Audit-SFP, Backup SFP and Crypto-SFP, to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

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

9.3.6.5 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.

Application note:

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

9.3.6.6 Management of TSF data (FMT_MTD.1/USER_CRYPTO)

FMT_MTD.1.1/USER_CRYPTO

The TSF shall restrict the ability to change default and delete the Identity and RAD for user with role attribute Crypto-officer and Crypto-user to Crypto-officer.

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

FMT_MTD.1.1/USER_AUDIT

The TSF shall restrict the ability to change default and delete the Identity and RAD for user with role attribute Auditor to Auditor.

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

FMT_MTD.1.1/RAD

The TSF shall restrict the ability to modify the RAD to its owner (i.e. Crypto officer, Crypto user or Auditor).

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

FMT_MTD.1.1/AUDIT

The TSF shall restrict the ability to query the audit data of the TSF required by FAU_GEN.1 to Auditor.

9.3.6.10 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

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

1) User management (FMT_MSA.1/ROLE_CRYPTO, FMT_MSA.1/ROLE_AUDIT, FMT_MTD.1/RAD, FMT_MTD.1/USER_CRYPTO and FMT_MTD.1/USER_AUDIT),

2) Management of audit data (FMT_MSA.3, FMT_MTD.1/AUDIT),

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

9.3.6.11 Security roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the roles Crypto-officer, Crypto-user and Auditor.

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 signing of DTBS by the cryptographic module.

9.3.7 Privacy (FPR)

9.3.7.1 Unobservability (FPR_UNO.1/CRYPTO)

FPR_UNO.1.1/CRYPTO

The TSF shall ensure that Anybody are unable to observe the operation

- Key generation (FCS_CKM.1),
- Signature creation (FCS_COP.1/SIGN),

- Key destruction (FCS_CKM.4)

on CSP SCD by Crypto-officer, Crypto-user or Auditor.

Application note:

The TSF requires the TOE to prevent side-channel attacks against the R.CSP-SCD, R.BACKUP_KEY 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 CSP to prevent any remaining side channels by appropriate security measures in the TOE environment.

The TSF requires the TOE to prevent side-channel attacks against the R.CSP-SCD through the intended output data of the TOE e.g. the random padding bits in the signature may contain information about the R.CSP-SCD if both are generated by the same pseudo-random number generator.

9.3.7.2 Unobservability (FPR_UNO.1/BACKUP)

FPR_UNO.1.1/BACKUP

The TSF shall ensure that anybody is unable to observe the operation

- Key entry (FCS_CKM.2)
- Key destruction (FCS_CKM.4)
- 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),

on R.BACKUP_KEY by Crypto officer, Crypto user or Auditor.

Application note:

The TSF requires the TOE to prevent side-channel attacks against the R.CSP-SCD, R.BACKUP_KEY 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.

9.3.8 Protection of the TOE Security Functions (FPT)

9.3.8.1 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_TST.1.

Refined by adding:

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

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

FPT_ITC.1.1

The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorized disclosure during transmission.

Application note:

FPT_ITC.1 addresses the confidentiality protection of the TSF data if they are exported as part of the backup data.

9.3.8.3 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 another 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 another trusted IT product and perform alarm indication to the Crypto-officer if modifications are detected.

Application note:

FPT_ITI.1 addresses the integrity protection of the TSF data if they are imported as part of the backup data and of the firmware updates.

9.3.8.4 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 Crypto Officer or Auditor 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 notification about detected physical attacks may be given e.g. through functional interfaces (stopping any other services but alarm signalization), acoustic or optic signals. The TOE non-IT environment should ensure that notification about physical tampering attempts given by the TOE shall be noticed by the CSP security personnel.

9.3.8.5 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 R.CSP-SCD, R.BACKUP_KEY (FCS_CKM.1)

— creates the signature with R.CSP-SCD (FCS_COP.1)

— stores R.CSP-SCD

— creates the cryptographic checksum of backup data and encrypts backup data with R.BACKUP_KEY (FCS_COP.1.1/BACKUP_ENC, FCS_COP.1.1/BACKUP_INT)

— stores other secret or private keys

by responding automatically such that the SFRs are always enforced.

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 R.CSP-SCD in case of loss of power. The TOE 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 R.CSP-SCD will prevent the use of an attacked TOE for signing until restoring the operational state.

9.3.8.6 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.

9.3.8.7 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 authorized user, during installation and maintenance to demonstrate the correct operation of the TSF.

FPT_TST.1.2

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

FPT_TST.1.3

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

Refined by adding:

The TSF shall perform self-tests

a) **Initialization**

   1) Extended software/firmware integrity test

b) **Power-Up Tests**

   1) Software/firmware integrity test

   2) Internal TSF data integrity test

   3) Cryptographic algorithm tests

   4) Random number generator tests

   5) Critical functions tests

c) **Conditional Tests**

   1) Pair-wise consistency test (for public and private keys).

   2) Manual key entry test (if manual key entry is implemented).

   3) 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 R.CSP-SCD (see FCS_CKM.1 and FCS_RND.1), cryptographic keys or parameters. If any critical function is not covered by these tests the TSF should implement additional self-tests.

The pair-wise consistency test for public and private keys may detect errors in the key generation process. Other consistency tests may check the correctness of the signing process and other cryptographic processes to prevent e.g. differential fault attacks. Manual key entry test may detect errors to prevent use of incorrect keys if manual key entry is implemented.

Continuous random number generator test may detect failure in operation of the generator to prevent use of wrong random number.

The TOE shall verify the integrity and authenticity of the TSF executable code at installation, maintenance and initialization to prevent malicious software running on the TOE.

9.3.9 Trusted path (FTP) — Trusted path (FTP_TRP.1)

FTP_TRP.1.1

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

FTP_TRP.1.2

The TSF shall permit local users to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for initial user authentication (FIA_UID.1, FIA_UAU.1) and TSF management (FMT_MSA.1/ROLE, FMT_MTD.1/USER_CRYPTO, FMT_MTD.1/USER_AUDIT, FMT_MTD.1/RAD, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1/ACCESS, FMT_MTD.1/AUDIT, FMT_SMR.1).

9.4 Security Assurance Requirements

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

Assurance Class	Assurance Component
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

Figure 2 — Security Assurance Requirements table

9.5 Security Requirements Rationale

9.5.1 Security Problem Definition coverage by Security Objectives

9.5.1.1 General

The following table presents the correspondence between the security objectives for the TOE and for its operational environment, and the Threats, Assumptions and organizational security policies.

	O.Audit	O.CSP-SCD_Secure	O.BACKUP_KEY_Secure	O.Check_Operation	O.RBAC	O.Attack_Response	O.Secure_State	O.Protect_Exported_Data	O.Sign_Secure	O.Backup_Secure	O.User_Authentication	OE.Application	OE.Audit	OE.Secure_channel	OE.Personnel	OE.Protect_Access	OE.Recovery	OE.Secure_Init	OE.Secure_Oper
T.BACKUP_KEY_Alteration			X	X		X	X									X		X	
T.BACKUP_KEY_Derive			X							X						X			
T.BACKUP_KEY_Disclose			X							X						X		X	
T.CSP-SCD_Alteration		X		X		X	X									X		X	
T.CSP-SCD_Derive		X							X							X			
T.CSP-SCD_Disclose		X						X	X							X		X	
T.CSP-SVD_Alteration								X											
T.Bad_SW	X			X	X		X				X	X	X	X	X	X			
T.Backup	X			X	X		X	X			X	X	X		X		X		
T.Data_Manipul												X		X					
T.Insecure_Init	X			X	X		X				X	X	X	X	X	X		X	
T.Malfunction	X			X			X						X		X	X	X		
T.Phys_Manipul	X			X		X	X						X		X	X			
T.KeyGeneration_Misuse	X				X						X	X	X		X	X			X
T.Signature_Misuse					X						X	X		X	X	X		X	X
T.Signature_Forgery									X										
P.Algorithms		X	X	X				X	X	X	X			X					
A.Trusted_Environment																X			X
A.Audit_Support												X	X		X				
A.Correct_DTBS												X		X					X
A.Data_Store															X		X	X	X
A.Secure_Channel														X					
A.CryptoUser_Agent												X							

Figure 3 — Security Objectives table

The following paragraphs provide the rationale between Security Objectives versus Threats, OSP and Assumptions.

9.5.1.2 Coverage rationale for Threats

T.BACKUP_Key_Alteration

The TOE shall ensure integrity of R.BACKUP_KEY (**O.BACKUP_KEY_Secure**). This is partially achieved with a nominal initialization of R.TSF_Data (**OE.Secure_Init**). During normal operation, integrity of cryptographic material shall be check by the TOE (**O.Check_Operation**). Alteration of R.BACKUP_KEY might come from a physical attack. Therefore, if such a data alteration arises, the TOE shall detect the attack, respond (**O.Attack_Response**) and jump to a secure state (**O.Secure_State**) to prevent loss of confidentiality from secret elements. To lower the risk of physical attack, the TOE shall be used in a secure place (**OE.Protect_Access**).

T.BACKUP_KEY_Derive

The algorithms and processes that are used for the cryptographic checksum or encryption operations shall not leak information that might help to derive R.BACKUP_KEY (**O.BACKUP_Secure**). This means that the backup data involved in the electronic signature shall not embed information about the secret elements (**O.BACKUP_KEY_Secure**). To lower the risk of accessing the TOE for observation and derivation of secret, the TOE shall be installed in a secure environment (**OE.Protect_Access**).

T.BACKUP_Key_Disclose

The TOE shall ensure integrity and confidentiality of R.BACKUP_ KEY (**O.BACKUP_ KEY_Secure**). Moreover, the cryptographic checksum operation itself shall not leak information about R.BACKUP_ KEY (**O.BACKUP_Secure**). In order to proceed to a secure checksum and encryption operations, procedures and controls in the TOE environment shall be defined and applied (**OE.Secure_Init**).

The TOE is protected by physical, logical and organizational protection measures, in order to prevent any protected assets disclosure (**OE.Protect_Access**).

T.CSP-SCD_Alteration

The TOE shall ensure integrity of R.CSP-SCD (**O.CSP-SCD_Secure**). This is partially achieved with a nominal initialization of R.TSF_Data (**OE.Secure_Init**). During normal operation, integrity of cryptographic material shall be check by the TOE (**O.Check_Operation**). Alteration of R.CSP-SCD might come from a physical attack. Therefore, if such a data alteration arises, the TOE shall detect the attack, respond (**O.Attack_Response**) and jump to a secure state (**O.Secure_State**) to prevent loss of confidentiality from secret elements. To lower the risk of physical attack, the TOE shall be installed in a secure environment (**OE.Protect_Access**).

T.CSP-SCD_Derive

The electronic signature algorithm and process that are used for the signature operation shall not leak information that might help to derive R.CSP-SCD (**O.Sign_Secure**). This means that every data involved in the electronic signature (R.DTBS, R.CSP-SCD or even signed data) shall not embed information about the secret key (**O.CSP-SCD_Secure**). To lower the risk of accessing the TOE for observation and derivation of secret, the TOE shall be used in a secure place (**OE.Protect_Access**).

T.CSP-SCD_Disclose

The TOE shall ensure integrity and confidentiality of R.CSP-SCD (**O.CSP-SCD_Secure**). Moreover, the electronic signature operation itself shall not leak information about R.CSP-SCD (**O.Sign_Secure**). Of course, the TOE shall not export R.CSP-SCD without protecting its confidentiality (**O.Protect_Exported_Data**). The TOE is protected by physical, logical and organizational protection measures, in order to prevent any protected assets disclosure (**OE.Protect_Access**).

In order to proceed to a secure electronic signature operation, procedures and controls in the TOE environment shall be defined and applied that allow secure key generation (**OE.Secure_Init**).

T.CSP-SVD_Alteration

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 (**O.Protect_Exported_Data**).

T.Bad_SW

Only Crypto-Officer role can perform firmware update (**O.RBAC**). Therefore a reliable authentication shall be done to ensure that user's identity (**O.User_Authentication**) is associated with the Crypto-Officer role. This association is performed by the client application (**OE.Application**). Crypto-Officer shall be aware of the consequences of his acts and trained (**OE.Personnel**). This kind of operation can have an important security impact on the TOE and its lifecycle. This is the reason why it shall be logged for future audit (**O.Audit**). The operational environment of the TOE shall provide technical solutions for audit storage and edition (**OE.Audit**).

The data uploaded in the TOE (firmware update files) shall be authenticated and verified in integrity (**O.Check_Operation**) before being installed in the TOE. These data shall be uploaded through a secure channel (**OE.Secure_Channel**) to lower the risk of distant software attack via the communication port of the TOE. In case of error during the update, the TOE shall return to a secure state, i.e. not applying the patch or step to a secure blocked state (**O.Secure_State**). Finally, the protected TOE environment (**OE.Protect_Access**) prevents any TOE modification by unauthorized people.

T.Backup

Backup and Restore operations shall be auditable events, recorded in a secured log file (**O.Audit**). Backup data are protected in authenticity and integrity (**O.Check_Operation**). Only the role Crypto-officer (**O.RBAC**) shall perform these operations after identification of the user (**O.User_Authentication**) based on a reliable client application (**OE.Application**). Auditor has access to previous restore and backup operations by analysis of stored audit logs (**OE.Audit**)

The data export mechanism shall use adequate confidentiality and integrity cryptographic mechanisms to prevent any tampering over backup data (**O.Protect_Exported_Data**). Recovery plans and procedures shall present the correct usage of backup data and describe backup and restore operations (**OE.Recovery**). Personnel shall be trained to perform these tasks (**OE.Personnel**). In case of error detection during a restore operation, the TOE shall enter a secure state (**O.Secure_State**).

T.Data_Manipul

Applications that use the TOE shall perform the necessary security checks on the data passed to the TOE (**OE.Application**). Nevertheless, the threat can also come from the outside world and therefore, a secure channel shall be set between the client application and the TOE (**OE.Secure_Channel**).

T.Insecure_Init

TOE initialization with insecure R.TSF_DATA can lower the security level of the TOE. Therefore, activities on the TOE shall be secured by a user authentication (**O.User_Authentication**). This Authentication is performed by the client application (**OE.Application**) that checks if the authenticated user is associated with a profile (**O.RBAC**) that is allowed to perform the initialization operation. Critical operation such as TOE initialization shall be log (**O.Audit** + **OE.Audit**) and initialization data shall be uploaded securely into the TOE (**OE.Secure_Channel**) and verified by the TOE before being validated inside the TOE (**O.Check_Operation**). If a problem arses during the initialization, the TOE shall jump or remain in a secure state (**O.Secure_State**).

Of course, personnel that operate the TOE, shall be aware of civil, financial and legal responsibilities, and trained (**OE.Personnel**), and they should apply the procedures and controls that allow to securely set-up and initialize 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 (**OE.Secure_Init**).

Finally, the protected TOE environment (**OE.Protect_Access**) prevents any TOE modification/initialization by unauthorized people.

T.Malfunction

Malfunction shall be detected by monitoring operation of the TOE (**O.Check_Operation**). If a malfunction arises, it shall be recorded (**O.Audit**) for future exploitation by maintenance services, and eventually compared with previous log files (**OE.Audit**). In case of malfunction, the TOE shall jump to a secure state (**O.Secure_State**). If a malfunction arises, personnel shall behave adequately (**OE.Personnel**) and set up a recovery solution (**OE.Recovery**) to avoid service discontinuity. To lower the risk of voluntary physical destruction of the TOE, the TOE shall be used in a secure place (**OE.Protect_Access**).

T.Phys_Manipul

Physical manipulation (box opening, penetration of secure area of the TOE) of the TOE could lead to a loss of confidentiality or integrity of the R.CSP-SCD. Personnel that handle the TOE shall be aware of this risk (**OE.Personnel**). Therefore, the TOE shall prevent tampering by detecting physical manipulation by entering a secure state (**O.Secure_State**) or even destroy R.CSP-SCD (**O.Attack_Response**). Physical manipulation can be also detected by a loss of integrity of critical data, therefore they need to be regularly check (**O.Check_Operation**). To prevent physical manipulation, the TOE shall be placed in a secure place (**OE.Protect_Access**) and every physical manipulation shall be logged (**O.Audit**) and logs shall be kept and made available by the environment (**OE.Audit**).

T.KeyGeneration_Misuse

The TOE can generate R.CSP-SCD/SVD pair. This critical operation shall be performed by authorized personnel (**O.User_Authentication**) with a Crypto-Officer role (**O.RBAC**) and relies on the client application (**OE.Application**). This operation shall be log for accountability (**O.Audit**) and kept available by the environment (**OE.Audit**).

Only trusted personnel should access the Crypto-Officer role (**OE.Personnel**) and they will have to follow procedures and controls in the TOE environment that allow operating the TOE within a CA system (**OE.Secure_Oper**).

NOTE The CA system will comply with the requirements of the EU Directive.

To lower the risk of TOE misusage, the TOE shall be operated in a secure place (**OE.Protect_Access**).

T.Signature_Misuse

This threat deals with personnel that use the TOE signature creation function without proper authorization. Therefore, the TOE shall only allow identified (**O.User_Authentication**) authorized (**O.RBAC**) and trained (**OE.Personnel**) personnel to perform the signature operation. This relies on the Client Application (**OE.Application**), its capability to connect securely to the TOE (**OE.Secure_Channel**) and accuracy of roles defined in the TSF Data (**OE.Secure_Init**). These operations shall be conducted within a CA system (**OE.Secure_Oper**).

NOTE The CA system will comply with the requirements of the EU Directive.

Finally, yo lower the risk of TOE misusage, the TOE shall be operated in a secure place (**OE.Protect_Access**).

T.Signature_Forgery

This threat deals with the risk 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 without knowledge of the R.CSP-SCD. Therefore, the TOE shall performed secured signature operations that counter this specific threat (**O.Sign_Secure**).

9.5.1.3 Coverage rationale for Organizational Security Policy

P.Algorithms

Cryptographic operations performed by the TOE shall comply with European and National regulations on cryptography. Operations are:

— electronic signature (**O.Sign_Secure**);

— confidentiality of secret data (**O.CSP-SCD_Secure, O.BACKUP_KEY_Secure**);

— authenticity and integrity check of firmware update (**O.Check_Operation**);

— export data protocols (**O.Protect_Exported_Data**) and backup operation (**O.Backup_Secure**);

— user authentication (**O.User_Authentication**);

— secure channel creation/support for the external application (**OE.Secure_Channel**).

Regarding signature creation, the set of algorithms for secure signature-creation devices and parameters for algorithms for secure signature-creation devices is provided in a separate document, ETSI/TS 102 176.

9.5.1.4 Coverage rationale for Assumptions

A.Trusted_Environment assumes that the operational environment of the TOE is secure (**OE.Protect_Access**). A set of operational procedures shall be in place for the organization operating the TOE within a CA system (**OE.Secure_Oper**).

NOTE The CA system will comply with the requirements of the EU Directive.

A.Audit_Support assumes that audit capabilities of the TOE will be exploited usefully by Auditors that are trained and aware of their responsibilities (**OE.Personnel**) thanks to a trusted Client Application (**OE.Application**) and the whole operational system that make the TOE audit trails available (**OE.Audit**)

A.Correct_DTBS assumes that the operational environment of the TOE provides integrity to the data to be signed. This assumption relies on the Client application (**OE.Application**) and its capability to establish a secure communication channel with the TOE (**OE.Secure_Channel**). A set of operational procedures shall be in place for the organization operating the TOE within a CA system (**OE.Secure_Oper**).

NOTE The CA system will comply with the requirements of the EU Directive.

A.Data_Store assumes that a set of operational procedures shall be in place for the organization operating the TOE within a CA system (**OE.Secure_Oper**).

NOTE The CA system will comply with the requirements of the EU Directive.

This induces also that personnel perform their tasks efficiently (**OE.Personnel**) and that in case of trouble backup will allow a quick restart of the system (**OE.Recovery**) and that secure initialization procedure will be followed (**OE.Secure_Init**) during the recovery.

A.Secure_Channel assumes that the client application provides a secure channel for authentication and management service of the TOE (**OE.Secure_Channel**).

A.CryptoUser_Agent assumes that the only crypto user is the client application, and that it performs efficiently the user authentication operations for the Crypto-User role (**OE.Application**).

9.5.2 Security Objectives coverage by SFRs

	O.Audit	O.CSP-SCD_Secure	O.Backup_Key_Secure	O.Check_Operation	O.RBAC	O.Attack_Response	O.Secure_State	O.Protect_Exported_Data	O.Sign_Secure	O.Backup_Secure	O.User_Authentication
FAU_GEN.1	X			X				X			X
FAU_GEN..2	X							X			
FAU_STG.2	X										
FCS_CKM.1		X	X								
FCS_CKM.2		X	X					X			
FCS_CKM.4		X	X			X	X				
FCS_COP.1 / SIGN		X							X		
FCS_COP.1 / BACKUP_ENC			X					X		X	
FCS_COP.1 / BACKUP_INT			X	X				X		X	
FCS_RND.1		X		X							
FDP_ACC.1 / CRYPTO		X			X						
FDP_ACC.1 / AUDIT	X				X						
FDP_ACC.1 / BACKUP			X		X			X		X	
FDP_ACF.1 / CRYPTO		X			X						
FDP_ACF.1 / AUDIT	X				X						
FDP_ACF.1 / BACKUP			X		X			X		X	
FDP_BKP.1								X			
FDP_ETC.1								X			
FDP_RIP.1		X	X			X	X				
FDP_SDI.2		X	X	X			X				
FIA_AFL.1											X
FIA_ATD.1											X
FIA_SOS.1				X							X
FIA_UAU.1											X
FIA_UID.1											X
FMT_MSA.1 / ROLE_CRYPTO					X			X			
FMT_MSA.1 / ROLE_AUDIT					X						

	O.Audit	O.CSP-SCD_Secure	O.Backup_Key_Secure	O.Check_Operation	O.RBAC	O.Attack_Response	O.Secure_State	O.Protect_Exported_Data	O.Sign_Secure	O.Backup_Secure	O.User_Authentication
FMT_MSA.2					X						
FMT_MSA.3					X			X			
FMT_MTD.1 / ACCESS_CONTROL					X						
FMT_MTD.1 / USER_CRYPTO											X
FMT_MTD.1 / USER_AUDIT											X
FMT_MTD.1 / RAD											X
FMT_MTD.1 / AUDIT	X				X			X			
FMT_SMF.1	X				X						X
FMT_SMR.1					X						
FPR_UNO.1/CRYPTO		X							X		
FPR_UNO.1/BACKUP			X					X		X	
FPT_FLS.1							X				
FPT_ITC.1								X			
FPT_ITI.1	X			X				X			
FPT_PHP.2						X					
FPT_PHP.3		X	X			X					
FPT_RCV.1							X				
FPT_TST.1				X			X				
FTP_TRP.1											X

Figure 4 — Security functional requirements table

O.Audit (Audit record generation and export)

This objective addresses the generation and protection of audit data by the TOE.

The audit generation is implemented by **FAU_GEN.1** and **FAU_GEN.2** with the audit events matching the list in O.Audit. Additional audit is implemented by FAU_GEN.1 and FAU_GEN.2.

The TOE stores the audit data according to **FAU_STG.2** until the audit trail is exported upon request of the Auditor or Crypto-officer under control of **FDP_ACC.1/AUDIT**, **FDP_ACF.1/AUDIT** and **FMT_MTD.1/AUDIT**.

FMT_SMF.1 and **FMT_MTD.1/AUDIT** require management function for the audit. These management functions are provided to the Auditor only.

Inside the TOE, the integrity of the audit data will be ensured by **FAU_STG.2**.

O.CSP-SCD_Secure (secure generation and management of R.CSP-SCD)

This objective addresses the confidentiality and integrity of the R.CSP-SCD which shall be ensured during their whole life time. The cryptographic secure generation of R.CSP-SCD is ensured by **FCS_CKM.1** and **FCS_RND.1** as well as operation by **FCS_COP.1/SIGN** according to the list of approved algorithms and parameters. The confidentiality and integrity of the R.CSP-SCD will be protected by **FDP_RIP.1** and **FDP_SDI.2** during internal processing. **FCS_CKM.2** provides a secure management of R.CSP-SCD during CM set up and operation. **FCS_CKM.4** requires secure key destruction to prevent any misuse of R.CSP-SCD after operational life time. R.CSP-SCD management and operation is under access control of **FDP_ACC.1/CRYPTO** and **FDP_ACF.1/CRYPTO**. **FPR_UNO.1/CRYPTO** protects R.CSP-SCD against side-channels, as well as **FPT_PHP.3** requires physical protection over the components that manipulate R.CSP-SCD.

NOTE The special protection of the R.CSP-SCD is needed if it is exported by backup function. This is addressed by O.Protect_Exported_Data. FDP_BKP.1 will protect the confidentiality if the R.CSP-SCD (or any other cryptographic key) is exported. The complex protection of the R.CSP-SCD as most valuable asset requires a systematic and complete vulnerability analysis considering high attack potential by AVA_VAN.5

O.BACKUP_Key_Secure (secure generation and management of R.BACKUP_KEY)

This objective addresses the confidentiality and integrity of the R.BACKUP_KEY which shall be ensured during their whole life time. The cryptographic secure generation of R.BACKUP_KEY generation is ensured by **FCS_CKM.1** and **FCS_RND.1** as well as operation by **FCS_COP.1/BACKUP_ENC** and **FCS_COP.1/BACKUP_INT** according to the list of approved algorithms and parameters. The confidentiality and integrity of R.BACKUP_KEY will be protected by **FDP_RIP.1** and **FDP_SDI.2** during internal processing. **FCS_CKM.2** provides a secure management of R.BACKUP_KEY during CM set up and operation. The **FCS_CKM.4** requires secure key destruction to prevent any misuse of R.BACKUP_KEY after operational lifetime. The R.BACKUP_KEY management and operation is under access control of the **FDP_ACC.1/CRYPTO**, **FDP_ACF.1/CRYPTO** for the cryptographic material management **and FDP_ACC.1/BACKUP** and **FDP_ACF.1/BACKUP** for the backup operations. **FPR_UNO.1/BACKUP** protects R.BACKUP_KEY against side-channels as well as **FPT_PHP.3** requires physical protection over the components that manipulate R.BACKUP_KEY.

O.Check_Operation (check for correct operation)

This objective addresses regular checks to verify that its components operate correctly. This security objective is implemented in the TOE by **FPT_TST.1** (TSF Testing). If these tests detect an error the TOE will transit into a secure state (see O.Secure_State). **FAU_GEN.1** generates audit records about the test results of **FPT_TST.1** to inform the user (Auditor or Crypto-officer) about the performed self-tests and their results. The **FPT_TST.1** includes checks of the executable code. **FPT_ITI.1** detects modification upon TSF data (firmware update, backup …), and **FDP_SDI.2** monitors the integrity of stored data into the TOE. The quality of random numbers is managed by **FIA_SOS.1** for the authentication purposes and **FCS_RND.1** for generation of secret key material.

O.RBAC (Management and control of TOE services)

This objective 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),

with the roles Auditor, Crypto-officer and Crypto-user as defined by the **FMT_SMR.1**.

FMT_MSA.1/ROLE_CRYPTO, **FMT_MSA.1/ROLE_AUDIT**, **FMT_MSA.2**, **FMT_MSA.3**, **FMT_MTD.1/ACCESS_CONTROL**, **FMT_MTD.1/AUDIT** and **FMT_SMF.1** assign the management functions for the cryptographic operations to the Crypto-officer and audit functions to the Auditor.

FMT_MSA.1/ROLE_CRYPTO extends the Crypto-officer's management functions to backup and restore.

FMT_MSA.1/ROLE_CRYPTO, **FMT_MSA.1/ROLE_AUDIT** and **FMT_MSA.3** require the TSF to enforce the Audit-SFP, Backup-SFP and Crypto-SFP to provide restrictive default values for security attributes which may be changed by the Auditor and the Crypto-officer.

NOTE The user management is addressed by O.User_authentication.

O.Attack_Response (detection of physical attacks)

This objective addresses the detection of physical tampering attempts and the secure destruction of the R.CSP-SCD if such attempts are detected. The **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 OE.Protect_Access requires CSP security measures for physical protection of the TOE. In case of emergency, **FCS_CKM.4** will ensure a secure deletion of R.CSP-SCD and **FDP_RIP.1** prevents leakage of secret data after de-allocation (emergency erasing).

O.Secure_State (secure state in case of error)

This objective addresses a secure state and protection of R.CSP-SCD confidentiality whenever the TOE detects an error. **FPT_TST.1** requires tests for error detection and **FPT_FLS.1** enforces preservation of a secure state when errors are detected. If failures occur, R.SCP-SCD and other confidential secret and private keys are destroyed by **FCS_CKM.4** and **FDP_RIP.1** prevents leakage of secret data after de-allocation (emergency erasing). The **FPT_RCV.1** enforces a maintenance mode where the ability to return the TOE to a secure state is provided. **FDP_SDI.2** enforces a jump to a secure state in case of integrity error detection over user data stored in container controlled by the TSF.

NOTE OE.Recovery describes the related security measures in the TOE environment.

O.Protect_Exported_Data (protection of data exported by the TOE)

This objective 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. **FDP_ETC.1** implements the Crypto-SFP for all exported data. **FDP_BKP.1** enforces confidentiality and integrity protection of backup data. The backup and restoration of R.CSP-SCD, other user data and TSF data are described in **FDP_BKP.1**. The confidentiality and integrity protection of the TSF data as part of the backup data are implemented by **FPT_ITC.1** and **FPT_ITI.1**.

FDP_BKP.1 relies on the cryptographic functions implemented by the following SFR:

- **FCS_CKM.2** importation of the backup keys,
- **FCS_COP.1/BACKUP_ENC** encryption of backup data,
- **FCS _COP.1/BACKUP_INT** data integrity protection.

FDP_BKP.1 requires encrypting R.CSP-SCD and electronically exported keys if they are exported. The backup and restore TSF will be under access control required by **FDP_ACF.1/BACKUP** according to **FDP_ACC.1/BACKUP**. **FMT_MSA.1/ROLE_CRYPTO** and **FMT_MSA.3** extend the management functions of security attributes to the Backup_SFP. **FMT_MTD.1/AUDIT** restricts the ability to export the TSF

audit data to the Auditor role.. For user accountability, **FAU_GEN.1** and **FAU_GEN.2** enforces identification of the user when performing an export. **FPR_UNO.1/BACKUP** implements a protection against side-channels when performing an export of data, to prevent illicit information flow over, at least, R.CSP-SCD.

O.Sign_Secure (Secure advanced signature-creation)

This objective addresses the security of the signatures, i.e. the signature does not reveal the R.CSP-SCD and cannot be forged without knowledge of the R.CSP-SCD. **FCS_COP.1/SIGN** enforces the cryptographic security of signature with respect to **P.Algorithms**. **FPR_UNO.1/CRYPTO** prevents illicit information flow about the R.CSP-SCD through side-channels. AVA_VAN.5 requires covert-channel analysis and a systematic and complete vulnerability analysis considering high attack potential, because the signature-creation with R.CSP-SCD, especially for certificates, is the most important and critical service of the TOE.

O.BACKUP_Secure (confidentiality of the backup key during backup operations)

This objective addresses the security of the cryptographic operations (checksum and encryption) performed by the TOE over backup data, i.e. the checksum does not reveal the R.BACKUP_KEY and cannot be forged without knowledge of R.BACKUP_KEY on the one hand and the encryption does not reveal R.BACKUP_KEY and cannot be decrypted without knowledge of R.BACKUP_KEY. **FCS_COP.1/BACKUP_INT** implements the cryptographic security of the checksum for integrity and **FCS_COP.1/BACKUP_ENC** implements the cryptographic security for confidentiality, both with respect to the **P.Algorithms**. . The backup and restore operations are under access control of **FDP_ACC.1/BACKUP** and **FDP_ACF.1/BACKUP**. **FPR_UNO.1/BACKUP** prevents illicit information flow about R.BACKUP_KEY through side-channels.

O.User_Authentication (authentication of users interacting with the TOE)

This objective addresses user's identification and authentication before having access to the TOE protected assets. **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 OE.Application). **FIA_UID.1** enforces timing identification and **FIA_UAU.1** enforces timing authentication. **FIA_SOS.1** ensures the verification of the quality of the secret used for authentication and **FIA_AFL.1** protects the TOE against brute forcing the VAD. **FAU_GEN.1** enforces tracability for Identification or Authentication errors.

FTP_TRP.1 enforces a trusted path between the client application ant the TOE. **FMT_MTD.1/USER_CRYPTO, FMT_MTD.1/USER_AUDIT, FMT_MTD.1/RAD** and **FMT_SMF.1** provide management functions for identification.

The following actions are allowed to be performed on behalf of the user, 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),

— detection of physical tampering (FPT_PHP.2).

Therefore these actions support the TOE protection and shall not allow access to the TOE protected assets.

9.5.3 SFR Dependencies

9.5.3.1 Justification of unsupported dependencies

9.5.3.1.1 FAU_GEN.1 < > FPT_STM.1

FAU_GEN.1 uses sequence data, which may be a sequence number or reliable time stamp. If sequence number is used FPT_STM.1 is not needed. The application note directs the ST Editor to include FPT_STM.1 if reliable time stamp is used by the TOE.

9.5.3.1.2 FCS_CKM.2 < > FCS_CKM.1

Key entry requires key components for split knowledge procedures not generated by the TOE. This key material will be provided by the TOE environment (as required by OE.Recovery).

9.5.3.1.3 FCS_COP.1/X < > FCS_CKM.1

The backup key material will be provided by the TOE environment (as required by OE.Recovery).

9.5.3.1.4 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.

9.5.4 Rationale for SARs

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 specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions.

The TOE described in this protection profile is just such a product. Augmentation results from the selection of **AVA_VAN.5**.

9.5.5 AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE generates uses and manages the most sensitive data of the CSP – the R.CSP-SCD. Any loss of confidentiality or integrity of the R.CSP-SCD threatens the security of the certificates signed with this R.CSP-SCD and therefore the security of all signatures created with the SCD which correspond to the certificates.

The cryptographic security of the R.CSP-SCD/R.CSP-SVD pair generation and the signing with the R.CSP-SCD can be ensured only by the TOE itself. The TOE shall be free of any covert channel which might compromise the R.CSP-SCD. The TOE environment shall support the TOE in R.CSP-SCD protection against physical and some other attacks but cannot make up for TOE security. The protection of the R.CSP-SCD shall be solely and in tabloid form provided by the CM as part of the trustworthy system. The complex protection of the R.CSP-SCD requires a systematic and complete vulnerability analysis by SAR AVA_VAN.5. The TOE protecting the R.CSP-SCD as most valuable asset shall be shown to be highly resistant to penetration attacks.

Bibliography

[1] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures

[2] ISO/IEC 15408-1[2], *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[3] ISO/IEC 15408-2[2)], *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

[4] ISO/IEC 15408-3[2)], *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

2) The following are equivalent to the aforementioned ISO/IEC 15408 standards:

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

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

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

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.