www.arx.com

cosign by arx

Security Target
for
ARX CoSign

Evaluation according to Common Criteria EAL4+

Table of Contents

List of Tables

List of Figures

1 Security Target Introduction

This Security Target describes the security objectives and security requirements for ARX CoSign version 8.2. The specifications are consistent with the *Common Criteria for Information Technology Security Evaluation, Version 3.1 ([2], [3] and [4]).*

1.1 Security Target Reference

CoSign Security Target, Version 2.6, ARX team, 27 April 2016.

Document Identification: *CoSign-CC-ST-2-6.doc*

1.2 TOE Reference

CoSign version 8.2 displayed on the TOE Console as <**Version SW8.2 HW7.0**> or on the Touch Screen as <**Version SW:8.2 HW:8.0**>

Evaluated configurations for CoSign are:
1. PRIMARY-HIGH AVAILABILITY WITH KEY REPLICATION (HA-PRI-REPL-INC-SIGKEY)
2. ALTERNATE-HIGH AVAILABILITY WITH KEY REPLICATION (HA-ALT-REPL-INC-SIGKEY)
3. SEAL-PRIMARY-HIGH AVAILABILITY WITH KEY REPLICATION (SEAL-HA-PRI-REPL-INC-SIGKEY)
4. SEAL-ALTERNATE-HIGH AVAILABILITY WITH KEY REPLICATION (SEAL-HA-ALT-REPL-INC-SIGKEY)

1.3 TOE Overview

1.3.1 TOE TYPE

CoSign is a digital signature product intended to be used as a SSCD/QSCD or Qualified electronic Seal Creation Device in a secure operational environment. The CoSign appliance is a network attached appliance consisting of computer hardware, hardware for tamper resistance, hardened operating system and the CoSign server software
The TOE is the whole CoSign appliance.

1.3.2 TOE usage and major security features

CoSign enables users of organizations or other users' communities to easily incorporate a digital signature into any type of content such as documents or data.

The CoSign appliance handles user accounts. Each user account can include one or more signature keys (SCDs) and other information such as the graphical images of the user. All user accounts, keys and other user related information are kept inside the secured appliance.
No user, including the appliance administrator or any other administrator, can use other user's key for digital signature operation.

Upon a user requesting to use his/her keys (SCD) for digital signature operation, the user access the CoSign appliance though the network based on TLS protocol. The TLS protocol is used for any request sent to the CoSign appliance. Only after two factor authentication of the user, which is based on presenting a static password and a One-Time password, that is based on OTP device, the user can digitally sign using his/her personal signature key and its matched certificate.
It is possible to define a certain time period where after the two factor authentication it will be possible to sign several digital signature operations within the same application.

Remark: In the following paragraphs, it will be presented that CoSign can be installed as a Seal Creation Device. In this case only one factor, which is based on a static password, is required for producing a digital signature.

A regular user in CoSign is also named Signatory in this document.
In the case that CoSign is installed as a Seal Creation Device, a Signatory represents the creator of a Seal.

The CoSign appliance can be interfaced from an end-user's PC installed with the CoSign client software. The CoSign client will enable the end user to integrate the digital signature that was produced by the CoSign appliance into a document such as a PDF file, XML data or any other document or data type.

Multiple users can sign simultaneously from many PCs. Each user session is fully separated from other user sessions.
Also, it is possible to interface CoSign through REST (Representational State Transfer) interface. This interface is aimed for signatories to perform same operations as provided through a CoSign client installation.
Unless otherwise mentioned, all references to the CoSign client also include the REST based client.

For every user account the following sub-entities are managed:

- **Signature keys** – every signatory can manage several signature keys
- **Certificates** – each of the above signature key has its own related certificate
- **Graphical Images** – each signatory can manage several images as part of the user account. During a signature operation, the user can choose to incorporate a graphical image into the document. The graphical image as well as other textual information such as the signature time can be displayed in the signed document.

A user can be enabled or disabled. If the user is disabled, the user cannot login to the appliance and perform operations such as digital signature.

CoSign can be deployed in the following configuration:

High Availability configuration with replication of signatory's private keys

One Primary (in HA-PRI-REPL-INC-SIGKEY configuration) and one or more Alternates CoSign appliances (in HA-ALT-REPL-INC-SIGKEY configuration) are installed in the operational environment. The Primary CoSign appliance serves clients for the purpose of digital signature operation and it updates the Alternate CoSign appliances upon any change in the user account information. A replication of the signatory's private keys, their matching certificate and, also, signatories' graphical images from Primary to Alternates CoSign is allowed.
Similarly, if CoSign is deployed a Seal Creation Device, one Primary (in SEAL-HA-PRI-REPL-INC-SIGKEY configuration) and one or more Alternates CoSign appliances (in SEAL-HA-ALT-REPL-INC-SIGKEY configuration) are installed in the operational environment.
It is not possible to use a Primary CoSign in HA-PRI-REPL-INC-SIGKEY configuration with one or more alternate appliances in SEAL-HA-ALT-REPL-INC-SIGKEY configuration and analogously it is not possible to use a Primary CoSign in SEAL-HA-PRI-REPL-INC-SIGKEY configuration with one or more alternate appliances in HA-ALT-REPL-INC-SIGKEY configuration

The replication of information is always done via a dedicated channel between the primary CoSign appliance and its alternate appliances.
Application level security that is executed in the Primary Appliance and Alternate appliance make sure that information is not altered and that sensitive information is encrypted.

Follows a high level scheme that shows how external entities interact with the CoSign appliance.
Unless otherwise mentioned, all references to the CoSign Appliance in a High Availability deployment refer to the Primary CoSign in this environment.

The Signatory interacts with the CoSign appliance using the CoSign client for the purpose of certificate enrollment and later on for the purpose of digital signature operations.
The Signatory can interact with the CoSign Appliance also via a RESTful interface.
The administrator interacts with the CoSign appliance for a variant of administrative tasks.
In the following scheme, it is shown that the CoSign client interacts with the CoSign.
In following sections a detailed description of the TOE components and the interface between the external components will be described in detailed.

Deploying CoSign as a Seal Creation Device

CoSign can be deployed as a Seal Creation Device.
This typical deployment is used for applications or processes aimed for producing a company seal or digital signatures produced by a legal entity of the organization.
In general, in this type of system, the user of the system is also named signatory and represents a legal entity.
In this type of configuration, the authentication will be based only on a static password.

Backup of the CoSign Primary appliance

The CoSign Primary Appliance can be Backed Up securely to a file for the purpose of disaster recovery.
It is mandatory that backup files will be kept securely and can be accessible only to the Appliance Administrator.
Upon a disaster, a special restoration process can be performed to get to an operational state.
The Restoration operation is very similar to an installation process. In the case of restoration, a backup file as well as the backup token are used for installing the CoSign based on an existing backup token and users' database.

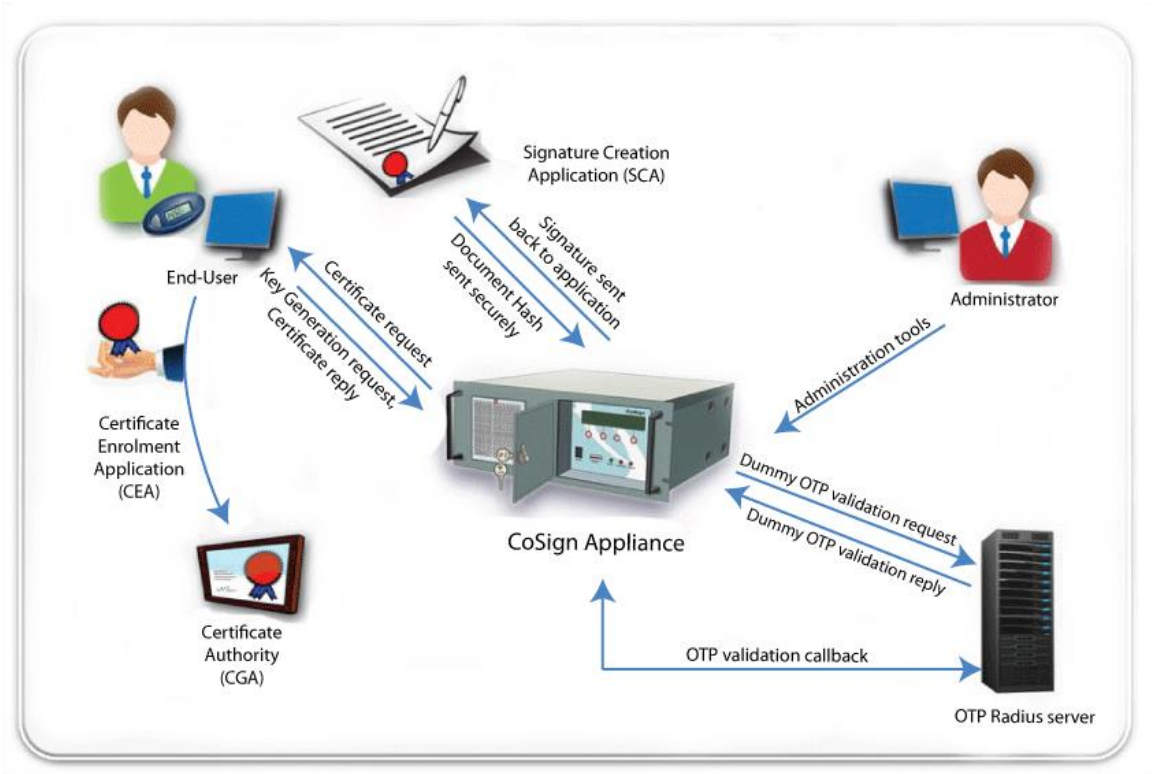

Figure 1 - CoSign High Level Design – Signature Creation Device

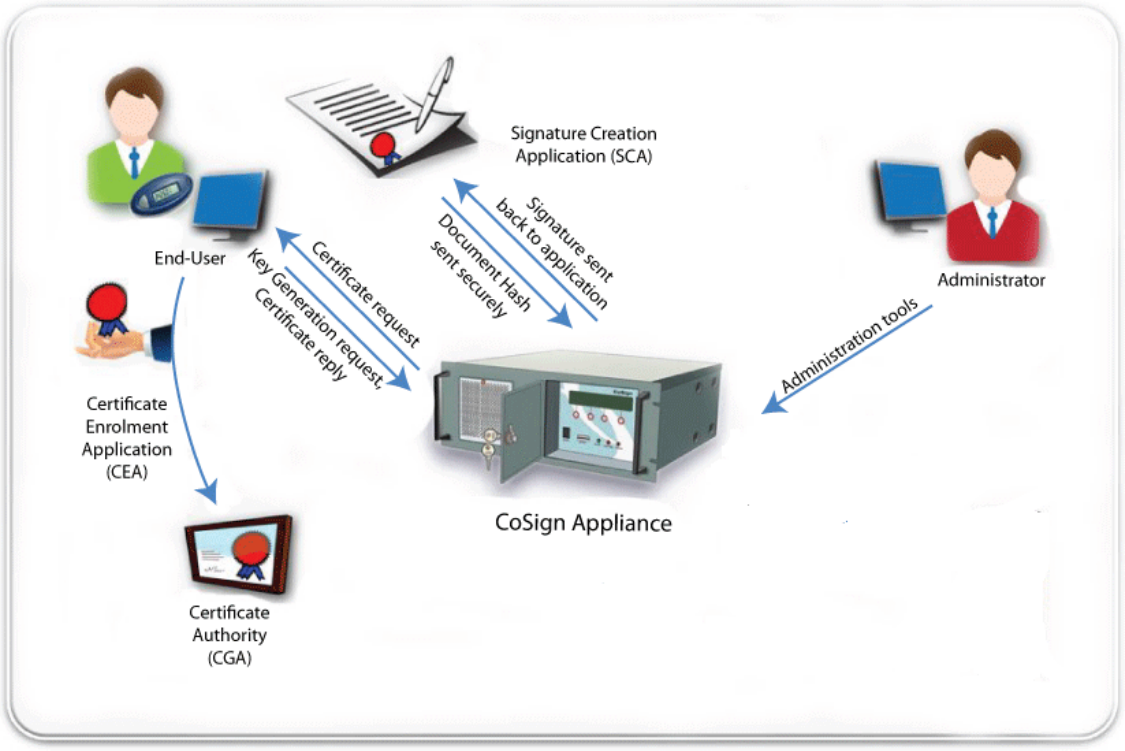

Figure 2 - CoSign High Level Design – Seal Creation Device

OTP Validation

The OTP validation process will be performed inside the CoSign appliance based on information that is stored inside an external OTP Radius server.
OTP validation is required only in the case that CoSign is deployed as a Signature Creation Device.
The flow of operation involves several steps:

1. Appliance receives the OTP in the above TLS session as part of the authentication phase prior to digital signature operation.
2. The OTP is stored internally in CoSign's memory. The appliance opens a Radius based communication with Radius Server [13]. The CoSign appliance sends a validation request based on a hash value of the OTP (Dummy OTP validation request).
3. The Radius Server gets the Dummy OTP validation request. Based on the user identity of the signatory inside the Dummy OTP validation request, OTP device profile is retrieved from the Radius Server's database.
4. The Radius Server opens a TLS based communication with the CoSign appliance sending the above Dummy OTP and the above OTP device profile. This communication will access the OTP validation callback service executed within the CoSign appliance.

5. The appliance will check the source of the communication and verify that it is the registered IP address of the Radius Server.
6. The OTP validation callback service will get the OTP device profile and the OTP kept inside the appliance memory and perform the OTP validation processing. Only if the OTP validation is successful, the internal memory of the appliance will mark the internal OTP as successfully validated.
7. In order to complete the technical flow of operation, the OTP validation callback will reply the Radius Server with the result of the OTP validation and the Radius Server will reply to the appliance back with the response to the Radius protocol.
8. The CoSign appliance will neglect this response and will use the internal OTP validation status, according to the status it will decide whether to continue with the digital signature operation or not.

1.3.3 Non-TOE hardware/software/firmware required by the TOE

The following non-TOE Hardware and Software are used in the operational environment:

- **OTP-Device**
  The OTP device hardware generates a dynamic password for the user. This dynamic password in combination with the user's static password is sent to the CoSign appliance for authentication. Only after proper authentication, the user can digitally sign.
  The OTP device should have tamper evidence mechanisms.
  OTP device is required only if CoSign is deployed as a Signature Creation Device.

- **OTP Radius Server**
  The CoSign appliance will interface the OTP Radius server through a Radius protocol [13].
  The OTP Radius server will callback the CoSign appliance to validate the One Time Password (OTP) based on OTP device profile kept inside the OTP Radius Server and the OTP provided by the signatory.
  The CoSign appliance will continue with the digital signature operation only upon a positive answer of the OTP validation performed by the OTP validation callback inside the CoSign appliance.
  OTP Radius device is required only if CoSign is deployed as a Signature Creation Device.

- **OTP-Device Profile**
  Information that is loaded to the OTP device and to the Radius Server. This

information is used by the OTP device to generate a new OTP or used by the Radius Server and the CoSign appliance for validating the given OTP.
The OTP-Device Profile can be uploaded to the OTP device either at manufacturing stage or at a later stage, depending on the OTP device technology and organizational policies.
The information must be loaded to the OTP device before the first usage.
OTP-Device Profile is required only if CoSign is deployed as a Signature Creation Device.

- **SCA (Signature Creation Application)**
  The SCA is an application that is executed in the user's PC. This application complements the CoSign appliance with a user interface with the purpose to create a digital signature. The SCA interacts with the CoSign appliance through the CoSign Client, which is installed in the user's PC as well.
  The SCA presents the data to be signed (DTBS) for review by the signatory, obtain prior to the signature process a decision by the signatory,
  if the signatory indicates by specific unambiguous input or action its intent to sign, the SCA sends a DTBS (Data To Be Signed) representation to the CoSign client and to the CoSign appliance, The CoSign clients requires a strong authentication prior to sending the DTBS-representation to the CoSign appliance.
  It is possible to configure CoSign to allow the signatory to multiply sign several documents or transactions within a fixed period of time after the two-factor authentication.
  The CoSign process the signature request and replies back with a digital signature.
  The replied digital signature will be replied back to the SCA, and the digital signature will be incorporated to the document by the SCA.
  The CoSign client installation include a software component called SAPI (Signature API), which enables SCAs to incorporate digital signatures into many type of documents standards such as PDF.
  In the case that CoSign's REST client is used, the interface allows sending the whole DTBS instead of the DTBS representation. For example, if the client wishes to sign a PDF file, the whole PDF file will be sent to the appliance. In this interface type there are some cases when the DTBS representation is sent to the appliance.
  The term DTBS/R will be used from now on to represent either sending the whole DTBS or DTBS-representation.
  The signature creation application is required to protect the integrity of the input it provides to the TOE signature-creation function as being consistent with the user data authorized for signing by the signatory. Unless implicitly known to the TOE, the SCA indicates the kind of the signing input (as DTBS/R) it provides and computes any hash values required.

- **CEA (Certificate Enrollment Application)**
  The CEA will request for a generation of a new signature key (SCD) inside the CoSign appliance and forward the returned certificate request to the CGA. The replied certificate will be incorporated to the account of the signatory in the CoSign appliance.
  It is possible to request for a qualified certificate, this means that all digital signature operations using the qualified certificate will be defined as qualified digital signature operation. Also, it is possible to request for an advanced certificate, this means that all digital signature operations using the advanced certificate will be defined as an advanced signature operation.

- **CGA (Certificate Generation Application)**
  The CGA generates certificates for users based on the signature key that is generated in the CoSign appliance.
  The CEA interfaces with the CGA. It sends the certificate request to the CGA and replies back with a certificate.

- **License USB Token**
  The License USB token is a Smart Card based USB token that includes license information protected with internal cryptographic means.
  The License USB Token is attached to the USB port of the Appliance.
  The information inside the License token is used by the appliance to impose restrictions, such as the maximal amount of allowed user account in the appliance.

- **Appliance Administrator PC/Laptop Web Console**
  Starting from CoSign Hardware version 8.0, the Appliance Admin Console's operation are based on a PC/Laptop that are connected to the dedicated network interface of the appliance.
  The administrative operations are perform through a Web based Console.

- **Special Routers in the operational environment**
  The operational environment can be equipped with special routing or switching technology that can be able to figure out automatically that the Primary CoSign Appliance does not provide service.
  This status is named Temporary fatal error to the Primary Appliance.
  In these cases that organization may require a partial service continuity that will enable the users the sign documents until the problem is resolved.
  In this case, the organization may use this special routing technology to forward the client-appliance secure communication to a selected alternate appliance.

This equipment will be configured back to use the Primary Appliance, when the temporary fatal error is resolved.

1.4 TOE Description

The following section will describe in details the CoSign digital signature solution.

1.4.1 High level description of CoSign

CoSign is a network attached appliance consisting of computer hardware, hardware for tamper resistance, Console (HW V7.0) or Touch Screen (HW V8.0), hardened operating system and the CoSign server software (figure 3).

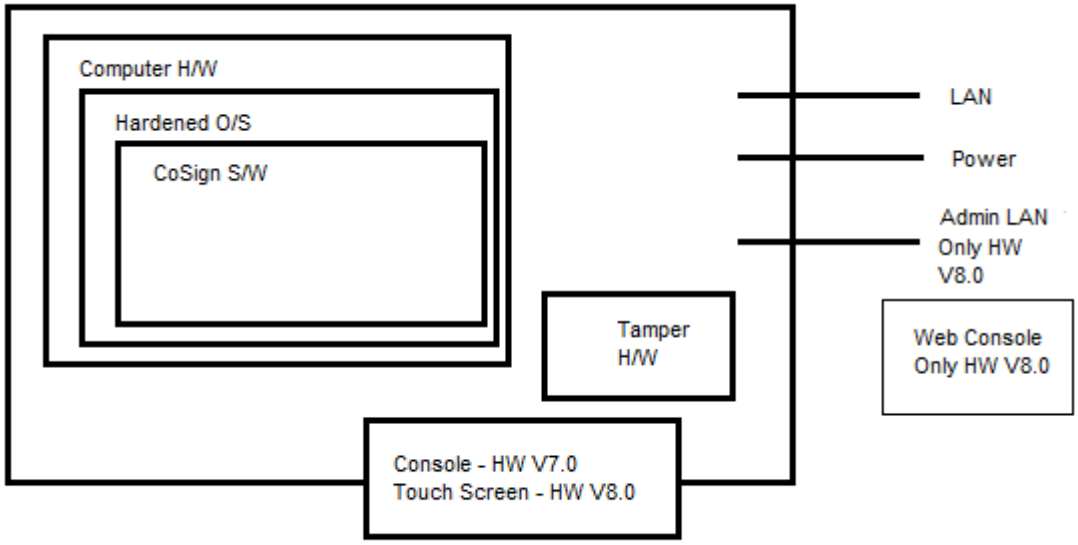

Figure 3 - CoSign internal design

The CoSign appliance is intended to be used as a digital signature product (SSCD/QSCD) within an organizational environment and should be physically installed in a secure environment in the organization's data center and connected to the organizational network.
A single CoSign appliance can securely manage many user accounts. More details about a user account initiation can be found in the following *Operational State* section.
In the case that CoSign is deployed as a Signature Creation Device, each user is provided with a One Time Password (OTP) device.

Each OTP device has its unique identification or unique OTP device profile.

When using an OTP device to authenticate a user, the user is requested to provide a password which is comprised of a static password and a dynamic password. The dynamic password is displayed by the OTP device. Without presenting a proper static and dynamic password, the user will not authenticate to the CoSign appliance.
The CoSign will validate the static password internally and will communicate with the OTP Radius server through the Radius protocol, then the OTP Radius server will communicate securely with the CoSign appliance as a callback for the purpose of validating the OTP. The OTP Radius server is located within the operational environment of the TOE.
For every user account, it is possible to generate several signature keys and their matching certificates.
If a user wished to digitally sign a document, the CoSign client will open a user session that is protected using a distinct secure channel using the TLS protocol Version 1.0 [8], Version 1.1 [17] Version 1.2 [15].

The TLS secure channel is based on TLS_RSA_WITH_3DES_EDE_CBC_SHA or TLS_RSA_WITH_AES_128_CBC_SHA256 mechanisms, where the symmetric key establishment is based on a 2048 RSA key, the symmetric encryption algorithm is based on 192 bit Triple Des EDE in CBC mode or AES-128 in CBC mode. The data integrity algorithm is based on SHA1 or SHA256 respectively. The confidentiality and integrity elements are compliant with ETSI TS 102 176-2, V. 1.2.1 (2005-07 [7]). In particular, the cryptographic functionalities that implement the secure channel (confidentiality and integrity protection) are compliant with [7] while the cryptographic functionalities involved in the secure channel establishment are different from the ones foreseen in [7] but, according to [12, tables 2 and 4] are equivalent from the point of view of the security level offered.

This secured communication channel is used for any request sent through the CoSign client.

Access to the user's signing key is only allowed after successful authentication. During authentication, the CoSign appliance will check the static password of the user and will interface the OTP Radius server to validate the OTP using the CoSign appliance callback. The digital signature output will be incorporated into the relevant document. OTP validation is required only if CoSign is deployed as a Signature Creation Device.
It is possible to configure CoSign to allow the user to multiply sign several documents or transactions within a fixed period of time after two-factor authentication.

The CoSign appliance maintains a cyclic Audit log that records all administrative functions, and every use of any user's signing key. The audit log cannot be erased and can be read only by an authorized administrator.

1.4.2 TOE definition

Figure 4 - CoSign Appliance Hardware version 8.0 - Front

Figure 5 - CoSign Appliance Hardware version 8.0 - Back

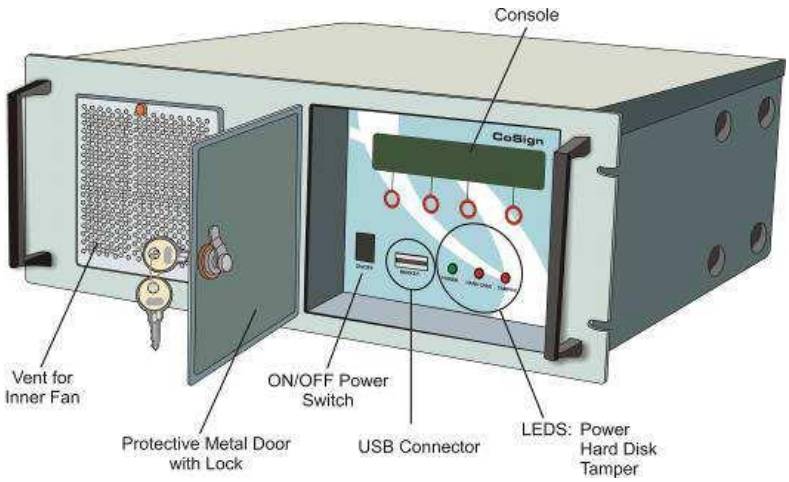

Figure 6 - CoSign Appliance Hardware version 7.0 - Front

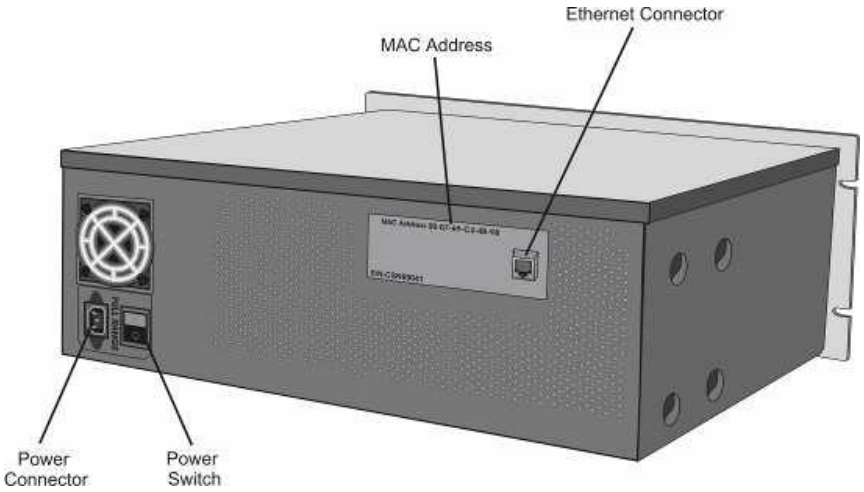

Figure 7 - CoSign Appliance Hardware version 7.0 - Back

The scope of the TOE is the whole CoSign appliance (see figures 4, 5, 6 and 7) including all appliance's hardware and software components.

1.4.2.1 Physical Scope of the TOE Hardware version 7.0

The appliance is a steel, rack mountable box. The physical interfaces of the appliance include the following elements:

- Network interface (Ethernet Interface using TCP/IP)

- Power switches (a front switch and a back master switch)
- Power connector
- LED indicators
- LCD display for displaying console information
- key pad with four buttons for administrative console operation
- A USB slot for a smartcard-based USB token
- One physical key slot and a physical key that can open and close a physical door that covers the above front power switch, LCD Display, LED indicators, key pad and the USB slot.

The internal hardware of the appliance includes:

- Motherboard and CPU
- A Hard disk that maintains the appliance's software and data
- A Tamper hardware device that automatically shut downs the appliance when trying to open the appliance. Also critical information, such as the critical master keys is deleted when a temper event occur.
- An internal smartcard based USB token that provides true random seed that is used for generating signature keys.
- Power supply and fans.

1.4.2.2 Physical Scope of the TOE Hardware version 8.0

The appliance is a steel, rack mountable box. The physical interfaces of the appliance include the following elements:

- Network interface (Ethernet Interface using TCP/IP)
- Network interface for Web Console administration
- Power switches (a front switch and a back master switch)
- Two Power connectors (Dual Power Supply)
- LED indicators
- Touch Screen for displaying console information
- A USB slot for a smartcard-based USB token

The internal hardware of the appliance includes:

- Motherboard and CPU
- Two SDDs that maintains the appliance's software and data
- A Tamper hardware device that automatically shut downs the appliance when trying to open the appliance. Also critical information, such as the critical master keys is deleted when a temper event occur.

- An internal smartcard based USB token that provides true random seed that is used for generating signature keys.
- Dual Power supply and fans.

1.4.2.3 Logical Scope of the TOE

When powering on the appliance, the CoSign appliance software is activated. The software is using a hardened Operating System.

If CoSign hardware version 8.0 is installed, through the appliance's touch screen it is possible viewing appliance's general parameters that are not security related. The appliance administrator can view the appliance's IP address, hardware version, software version etc.

If CoSign hardware version 8.0 is installed, through the Web based console that can be accessed only through the administrative network interface, the following operations can be performed:

- View appliance general parameters that are not security related. The appliance administrator can view the appliance's IP address, the amount of users, software version etc.
- Configuring networking related parameters.
- Resetting a tamper state after a tamper occurred.
- Setting the appliance to factory settings.
- Shutting down the appliance.
- Setting the appliance's current time.

If CoSign hardware version 7.0 is installed, through the appliance console the following operations can be performed:

- View appliance general parameters that are not security related. The appliance administrator can view the appliance's IP address, the amount of users, software version etc.
- Configuring networking related parameters.
- Resetting a tamper state after a tamper occurred.
- Setting the appliance to factory settings.
- Shutting down the appliance.
- Setting the appliance's current time.

The CoSign software includes several software modules that are aimed to enable end users to remotely access the appliance and perform a digital signature operation.

Accessing the appliance is done using a CoSign client software installed in the end user's PC and establishing a TLS session between the remote client and the CoSign appliance.

The digital signature command and the returned digital signature information will be passed to/from the CoSign using the established TLS session.

The CoSign software can be in either of the following states:

- Factory State – The state that the product arrived from the factory. The product is not installed yet and cannot be accessed by end users.
- Operation State – The product is installed and ready for managing new user accounts and performing digital signature operations.
- Tamper state – The appliance has been tampered with. At this state end users cannot perform any digital signature operation.

More information of the TOE states is described at the *CoSign deployment lifecycle* section.

While in operational state, the following sections describe the relevant services offered by the TOE.

1.4.2.3.1 Functional User operations

When the product is in its operation state, users can communicate securely with the appliance using TLS protocol over TCP/IP and perform the following operations:

RSA signature generation
A DTBS/R is sent to the TOE as part of a user session. The TOE performs a digital signature operation and replies with the digital signature.

RSA key generation
Generating a new RSA key. The generated signing key is performed internally inside the appliance. CoSign contains a hardware random generator which is based on a smartcard chip. Using a pseudo random generation (HMAC-DRBG – NIST SP 800-90A) [16], the required random for the key generation is provided. The RSA key generation algorithm is compliant with [5], [6] and [9]. The RSA key can be of one of the following size: 2048 bits or 4096 bits.

Managing graphical signatures
Each user can upload several graphical signatures to be contained inside the CoSign appliance database under the specific user's account. These images can

be fetched by the CoSign client and be incorporated as a visible signature into the signed document as part of the signature operation.

Managing Certificates
All users' certificates are also stored in the CoSign appliance database under the specific user's account.
There are two occasions that certificates are used by the user (signatory).

- Certificate enrollment
  During certificate enrollment, an RSA key is generated inside the CoSign appliance, a signed SVD is extracted from the CoSign appliance and sent to the CGA out of the scope of the TOE. The new certificate is uploaded back to the TOE.
- Signature Creation application (SCA)
  The signature generation application will retrieve all users certificate and let the user choose the required certificate for the digital signature operation.

1.4.2.3.2 CoSign random number generation

CoSign includes a built-in random number generation that is used in a large variety of operations such as signature key generation and other sensitive information as well as a set of critical keys, which are described in the next section.
The random generation is aligned with [6] and is based on using a both True Random number generation mechanism (trueran) and a pseudo-random (pseuran) number generation mechanism.
The true random generation mechanism is based on a true random seed given by an internal smart card chip in a form of a USB token.
The smartcard chip is based on the Atmel chip AT90SC25672RCT-USB with Athena IDProtect/OS755 Java Card.
This chip has a Common Criteria EAL 4+ certification.
The pseudo-random generation uses the above true random seed and calculates the random number using the deterministic algorithm described in [16].

1.4.2.3.3 CoSign Master Keys

CoSign uses the following critical Triple DES keys (192 bit length) that are generated during the appliance installation and are located in both volatile memory of the appliance and inside the internal tamper device:

- **SRV KEK – Master key used for AUK Keys encryption**
  This 192 bit critical data in conjunction with the static password of the user build a user specific KEK (Key Encryption Key).
  The user specific KEK encrypts/decrypts a randomly generated Account Unique Key (AUK).

The AUK is used to encrypt the signature keys that belong to the specific user account.
The SRV KEK encrypts graphical images and certificates inside the TOE database.

- **SRV Data Integrity – Master key used for MAC calculation/verification of users database records**
  This 192 bit critical key protects the integrity of all the user information, key information, other user objects and other sensitive information in the database of the CoSign appliance.
- **SRV backup Encryption – Master key used for Encryption of the CoSign backup**
  This 192 bit critical key encrypts the backup of the Primary CoSign Appliance. Information that is already encrypted (such as signature keys) are encrypted with this master key in addition to the already encrypted data (in this case, the encrypted keys).
- **SRV backup Integrity – Master key used for MAC calculation/verification of the CoSign backup**
  This 192 bit critical key protects the integrity of the backup of the CoSign appliance.

All generated critical keys use the appliance random generation mechanism, as defined in the above section.

All critical keys are also copied to a dedicated SmartCard based USB token for a backup purpose.
The backup USB token is prepared during the appliance installation and its secured information is copied to an additional dedicated USB token.
The backup USB tokens must be kept in a dedicated safe in the responsibility of a dedicated administrative personal.

The backup token is used in the following operations:

- **Reset Tamper**
  In the case of a tamper event, the appliance administrator can perform a reset tamper operation.
  The Appliance Administrator should perform the Reset Tamper operation only if he/she is absolutely certain that the appliance was opened in a control manner.
  In the case that the tamper event occurred as part of a security compromise, it is forbidden to perform the Reset Tamper operation due to the risk that bringing the appliance to a production state may compromise inner information such as the signatory's keys.
  In the case that the appliance administrator approves the Reset Tamper operation, the backup USB token is required since all above critical

information is wiped out from the tamper device and the only way to reconstruct the information is using the backup USB token. This operation is performed only from the Web based appliance's console when CoSign hardware version 8.0 is used or the Appliance's console when CoSign hardware version 7.0 is used.

- **Installation of an Alternate appliance**
  Making sure that the Alternate appliance is having the same critical keys as the keys that are used by the Primary appliance.
- **Restoration of the Primary appliance**
  In the case of a disaster. CoSign Backup file, together with the backup USB token can be used for recovering the Primary CoSign Appliance to operational state before the disaster occurred.

1.4.2.3.4 Functional Administrative operations

An Appliance Administrator can perform administrative tasks either through the Web based console based on the dedicated network interface (when CoSign Hardware version 8.0 is used) or through the TOE console (when CoSign Hardware version 7.0 is used) or using the secure CoSign Client-CoSign Appliance interface that is based on a secure network connection.

When CoSign hardware version 7.0 is used, console related operations do not required the appliance administrator's authentication and rely on the physical security of the operational environment of the TOE.

When CoSign hardware version 8.0 is used, any operation through the Web Console that updates parameters in the CoSign Appliance will require physical access to the CoSign Appliance and also performed from a dedicated network interface.

There are two types of administrators:

1. Appliance Administrator – installs the appliance and manages appliance related functionalities.
   Some of the appliance administrative functions are done using the Web based console (in the case that CoSign Hardware version 8.0 is used) or the TOE console (in the case that CoSign Hardware version 7.0 is used).
2. Users Administrators – manages user accounts

Here follows some of the operations that can be performed by the above administrators:

- A special users' administrator can perform User management operations (creating a new user account, a limited update of an existing user account, deleting an existing user account and viewing user information)

- The Appliance administrator can upload digitally signed software updates. The updated software will need to be also Common Criteria certified under this Security Target or an updated version of this Security Target.
- The Appliance administrator can download audit and debug logs
- The appliance administrator can upload the TLS Server key used for the secure channel of the REST interface.
- The appliance administrator can perform a backup operation.

For more information refer to section 7.1.

The following operations are performed automatically by the CoSign appliance in operational state:

- Tamper detection & protection when opening the appliance cover either with the appliance is on or off.
- Secure storage of signature keys
- Storage of application data (certificates and graphical signature images)

1.4.2.3.5 CoSign in High availability mode of work

General Description

It is possible to deploy two or more CoSign appliances in the same operational environment. The purpose of having more than one active appliance is to enable the organization's users to continue and digitally sign in the event of a hardware or software malfunction to the primary CoSign appliance.

The main CoSign appliance is named the Primary CoSign appliance, while the other CoSign appliances are named the Alternate CoSign appliances.
There are some Appliance Administrative operations that can be performed on an Alternate Appliance such as:

- Shutdown/Restart/Soft-Restart the appliance
- Download Appliance Audit Log
- Upload updated software
- Upload CoSign REST Server Key.
- Console based operations through CoSign Web Console (when CoSign Hardware version 8.0 is used) or TOE Console (when CoSign Hardware version 7.0 is used).
- Turning Alternate Appliance to a Primary Appliance

Signature keys as well as certificates and graphical images are replicated.

The security of the data replication is based on application level data integrity mechanisms where all security related information includes a MAC.

Sensitive information as the signatory keys or the graphical images is kept encrypted.

Only one CoSign appliance is marked as the Primary CoSign appliance.

Digital Signature operations and all management operations are allowed only using the Primary Appliance and not the Alternate Appliances, except for the case of temporary fatal error of the Primary Appliance.

The Operation Environment must be defined in a manner that signatory operations are forwarded to a selected Alternate Appliance only in the case that the Primary Appliance is not able to provide a service due to Temporary Fatal Error of the Primary Appliance.

A fatal error of the Primary appliance means that the appliance does not provide any service.
As an example, if the Appliance's power is down or there is critical networking service based problem, this will be considered as a temporary fatal error of the appliance.

When there are more than one alternate appliances in the operational environment, a specific alternate appliance will be defined, by the operational environment as the Alternate Appliance that can be used to provide partial service in the case of a temporary fatal error of the Primary Appliance.
This certain alternate appliance is required to be defined in advance, as part of the deployment of the set of CoSign Appliances.
In the case of only one Alternate Appliance in the operational environment, this Alternate Appliance can be used to provide partial service in the case of a temporary fatal error of the Primary Appliance.
The main functionality of the selected Alternate Appliance is to enable signer perform digital signature operation in the case of temporary fatal error of the Primary Appliance.

This operation can be done in an automatic manner using a smart router in the operational environment or any other networking related technology deployed in the operational environment.
The router can figure out that the Primary Appliance does not offer a service (for example, the Primary Appliance is not replying for any request) and by that decide to forward the communication to the selected alternate appliance.

When there is a technical resolution and the Primary Appliance is back in service, the above routing technology that is used by the operational environment (or any other technology), will forward requests sent by the clients to the Primary Appliance.

This will happen either when the Primary Appliance was recovered from the fatal error or in the case that there is another available Primary Appliance.

The available operations that can be provided by an Alternate Appliance are:
- Receive updates from the Primary Appliance – In the case that there is a Temporary Fatal Error for the Primary Appliance, there will be no updates received from the Primary Appliance.
- User/Signatory related operations – The operational environment will allow the following operations only in the case of a temporary fatal error of the Primary Appliance. Follows are the allowed operations:
    - Perform a signature operation
    - Get user graphical images
    - Get user certificates
    - Get user information
- There are no Users Administrator operations allowed for any Alternate Appliance
- Appliance Administration operations that can be performed upon an Alternate Appliance as described above.

Primary Appliance Recovery methods

If the temporary fatal error of the appliance cannot be resolved (i.e. a permanent fatal error), it is mandatory to recover a primary appliance with the most updated data of the previous Primary Appliance.

A new primary appliance can be recovered using one of the following ways:
- The appliance administrator will be able to turn one of the alternate appliances to act as the new primary appliance of the operational environment.
- A backup of the appliance can be restored to a new appliance that is in factory state.

1.4.2.3.6 CoSign appliance deployment Lifecycle

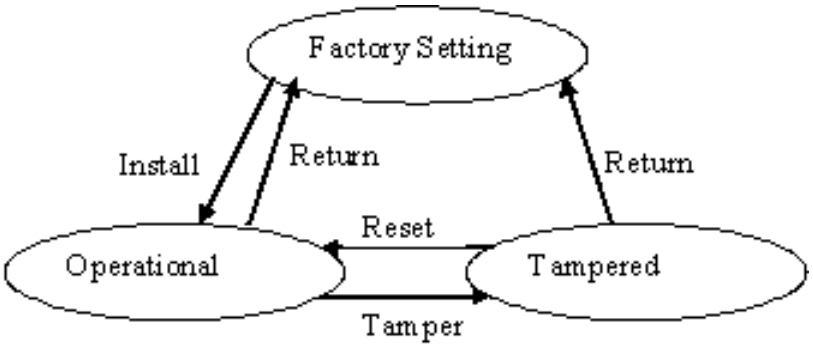

Figure 8 - CoSign deployment lifecycle

Figure 8 presents the complete product lifecycle where installation, return to factory setting and reset tamper are operations permitted to administrators, and tamper is an external tamper event. The factory setting and reset tamper operations are performed only from the Web Console of the appliance when CoSign hardware version 8.0 is used or the Appliance's console when CoSign hardware version 7.0 is used.
Follows is a more detailed description of these states.

Factory Settings state

In this state the CoSign appliance is not installed and there are no user accounts, signature keys or any other user info inside the CoSign database.

Change to Operational State

Only in this state the CoSign can be installed. During the installation, the CoSign appliance is configured according to customer's environmental definitions.
The installation of the CoSign shall be performed in a secure environment.
During installation, four master keys are generated that are used to protect the integrity of information such as the user accounts and internally take part in the encryption of the signature keys of the appliance. These master keys are kept in a dedicated USB token during installation and must be kept in a secure place such as a safe.
At the end of a successful installation, the CoSign is in operational state.

In the case of a restoration from backup the installation process is very similar. The backup USB token and its four master keys are used for the restoration process. Also, a secure backup file that includes the database information is

restored to the restored primary CoSign appliance.

High Availability

CoSign shall be installed in high availability mode, where the primary CoSign appliance will be installed in the manner stated above.
A special manual installation procedure should be executed upon each of the alternate appliances.
During installation of the alternate appliance:

- The appliance administrator is requested to provide the special backup token, so that the primary appliance and the alternate appliance share the same master keys.
- The IP address of the alternate appliance will be joined to the distribution list of alternate appliances that is managed in the primary appliance.

When the installation of the primary appliance is complete, the primary appliance is in the operational state. When the installation of an alternate appliance is complete, the alternate appliance is in the operational state.

Change to Tampered State

In this stage, the appliance will still be remained in a factory settings state, although it is recommended that if any physical tampering had occurred, the appliance administrator should be alerted.

Operational state

In this state, it is possible to create new user accounts and activate the account for starting to perform a digital signature operation.

A user account has the following lifecycle:

Creating of a new account

This operation is done by a *users administrator*.
During account creation, the users administrator can set an activation password for the user.
This password will be given to the end user either by a Pin Mailer or other mechanisms. These mechanisms are out of the CoSign scope.

Account activation by the end user

An account can be activated only once. During activation the user will need to provide the following details:

- Activation password as given by the users administrator
- Dynamic password as presented by the OTP device in the case that CoSign is installed as a Signature Creation Device and not as a Seal Creation Device.

- A new static password and a confirmation password

During activation, a new *Account Unique Key (AUK)* will be generated for the account and encrypted in the User Record in the database. The encryption key will be build using the CoSign first Master Key and the static password of the user.
The AUK is a three key Triple-DES key that is used for encrypting any future generated signature key of the user.
Only after a successful activating of the account the user can enroll for new signature keys or sign with existing signature keys.
If the account is already activated, the user must contact the organization immediately for a suspicion that the account was already misused. Any such event will be reported to the CoSign audit log.

It is not possible setting a new activation password for the user after the account was activated.
In the case that CoSign is deployed as a Signature Creation Device, It is forbidden replacing an OTP device or OTP device profile for a user after an account was activated, the user account must be revoked and a new account for the user should be created.

Operations for an activated account

The following operations can be performed by the signatory when the account is activated:

- Generating a new signature key and getting a certificate request for the newly generated key.
- Accepting a certificate for new signature key
- Getting a list of certificates for the account
- Managing graphical images for the account and getting a list of graphical images of the account.
- Digital signature operation
- Change password operation
  The user will provide the old static password as well as the new static password and a confirmation of the new static password.
  During this operation, the AUK of the user will be re-encrypted with a new KEK that is build from the first master key and the new static password.

Account revocation by a Users Administrator

At any point of time, the users' administrator can revoke an account. All signature keys, certificates and graphical images are deleted.
In the case that CoSign is deployed as a Signature Creation Device, it is forbidden to allocate the OTP device or OTP device profile to another user.

High Availability considerations
All management operations as well the signatory operations are done only by accessing the primary appliance. This includes: User account creation, account activation, changing static password.
If the Primary Appliance is not accessible, only user related operations can access the alternate appliance.
Also, the appliance administrator can download the audit log of the alternate appliance(s).
Also, the alternate appliance is used for disaster recovery purpose and/or business continuity purpose.

The primary appliance maintains a distribution list of all available alternate appliances. The primary appliance periodically replicates all the updates occurred to user accounts in the last few minutes. The replication is done to all alternate appliances in the distribution list.
If an alternate appliance is removed from the distribution list, no updated information will be sent this alternate appliance.

In the case of a disaster to the primary appliance, it is possible to change the role of an existing alternate appliance to take over to the role of a primary appliance. This is done using a special administrative action.

Change to Factory Settings State
An appliance can be returned to factory state by activating a special operation in the appliance's Web Console (in the case that CoSign hardware version 7.0 is used) or the appliance's Console (in the case that CoSign hardware version 8.0 is used) . This operation will destroy all user account information. The operation will also remove all master keys information from the tamper device.
Performing a reset to factory operation upon an alternate appliance is similar to performing a reset to factory operation upon a primary appliance.

Change To Tampered State
An appliance will enter to a tamper state in the event of tampering.

Tampered State
CoSign contains a tamper resistant mechanism which when activated actively erases the sensitive data in order to protect the user's signature keys.
In the Tamper state the appliance is not started and does not serve any request beside an approval of an appliance administrator of the tamper condition.

Change to Operational State
If the CoSign appliance was in operational state, only by using the special backup USB key, the appliance administrator can turn the appliance from the

tamper state to an operational state again. All Master key information will be copied from the special backup USB key into the appliances' tamper device.
If the CoSign appliance was in factory state, the reset tamper operation by an administrator will not require using the special backup USB token, and the appliance state will be changed back to factory state.
The Appliance Administrator should perform the Reset Tamper operation only if he/she is absolutely certain that the appliance was opened in a control manner. In the case that the tamper event occurred as part of a security compromise, it is forbidden to perform the Reset Tamper operation due to the risk that bringing the appliance to a production state may compromise inner information such as the signatory's keys.

The change of states is similar to primary and alternate appliances.

Change to Factory Settings state

An appliance can be returned to factory state by activating a special operation in the Appliance Web Console (when CoSign Hardware version 8.0 is used) or the Appliance's Console (when CoSign Hardware version 7.0 is used). This operation will destroy all user account information
Performing a reset to factory operation upon an alternate appliance is similar to performing a reset to factory operation upon a primary appliance.

2 Conformance Claim

CoSign Security Target and this TOE are conformant with version 3.1 revision 4 of the Common Criteria for Information Technology Security Evaluation:

- Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2012 Version 3.1 Rev. 4. CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2012 Version 3.1 Rev. 4. CCMB-20012-09-003

CoSign Security Target is conformant to assurance level EAL4 augmented with AVA_VAN.5, ALC_FLR.1 and ATE_DPT.2 defined in Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2012 Version 3.1 Rev. 4. CCMB-2012-09-003 (CC part 3)

CoSign Security Target is not conformant to any PP.

3 Security Problem Definition

The following chapter defines the security problems that need to be addressed as part of the TOE. The chapter will enumerate the Threats, OSPs and assumptions that relate to the Security problem definition.

3.1 Threats

This section will start with a list of assets and subjects of the TOE and end with the threat agents and threats to the assets.

Assets and objects:

1. SCD: private key used to perform a digital signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained. This restriction applies for any SCD of any signatory during the entire lifecycle of the TOE.
2. SVD: public key linked to the SCD and used to perform digital signature verification. The integrity of the SVD when it is exported must be maintained.
3. DTBS and/or DTBS/R: data-to-be-signed or data-to-be-signed representation, which the signatory intend to be sign. The representation is based on a hash value of the data. Their integrity and the unforgeability of the link to the signatory provided by the digital signature must be maintained.
4. Signature-creation function of the TOE to create digital signature for the DTBS/R with the SCD.
5. VAD: static password as well as OTP entered by the End User to authenticate the user prior to performing a signature creation operation or a seal creation operation.
   Remark: OTP is relevant if the TOE is installed as a Signature Creation Device.
6. RAD: Reference static password related information as well as OTP device serial ID or OTP device profile attached to the user and OTP device key material that is used to authenticate the user.
   Remark: OTP is relevant if the TOE is installed as a Signature Creation Device.
7. Generated digital signature.
8. Signatory's certificates: although these elements can be publicly available in signed document, only the signatory use his/her certificate as part of the digital signature ceremony, handled by the SCA.

9. Signatory's graphical images: although these elements can be extracted from the signed document, only the signatory use his/her graphical images as part of a digital signature ceremony handled by the SCA.
10. System Parameters and a variant of TOE internal data elements such as the internal list of alternate appliances. Some of the System parameters and other data are locked after the TOE installation. Other System parameters and TOE data can be modified only by the appliance administrator. Follows some of the System Parameters and data that are used by the TOE:
    - Radius Server IP address
    - List of alternate appliances
    - REST TLS Server key
    - Static password policy attributes

Users and subjects acting for users:

Subjects	Definition
S.User	End user of the TOE who can be identified as Users Administrator, Appliance Administrator or Signatory. In the TOE the subject S.User may act as S.ApplianceAdmin in the role R.Appliance Admin or as S.UserAdmin in the role R.UserAdmin or as S.Sigy in the role R.Sigy.
S.ApplianceAdmin	User who is in charge to perform the TOE initialization or TOE configuration.
S.UserAdmin	User who is in charge to managing users of the TOE. This account will be in charge of providing an activation password for the created users.
S.Sigy	User who uses the TOE for the purpose of digital signature operations. The user uses his/her account in the TOE on his own behalf or on behalf of the natural or legal person or entity he/she represents. In the TOE the subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as Signatory.

Threat agents:

S.ATTACKER	Attacker. A human or a process acting on his behalf being located outside the TOE. The main goal of the S.ATTACKER is

	to access the SCD or to falsify the digital signature. An attacker has a High attack potential and knows no secret.
S.INTERNAL	A human with high attack potential that has access to some of the secured information such as the activation password of the end user and tries to take advantage and perform a signature operation on behalf of a user of the appliance.

Follows a formal list of the inspected threats:

T.SCD_Divulg *Storing, copying, and releasing of the signature-creation data*

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature-creation in the TOE.

T.SCD_Derive *Derive the signature-creation data*

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

T.Hack_Phys *Physical attacks through the TOE interfaces*

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

T.SVD_Forgery *Forgery of the signature-verification data*

An attacker presents a forged SVD to the CGA. This result in loss of SVD integrity in the certificate of the signatory.

T.SigF_Misuse *Misuse of the signature-creation function of the TOE*

An attacker misuses the signature-creation function of the TOE to create digital signature for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.DTBS_Forgery *Forgery of the DTBS/R*

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

T.Sig_Forgery *Forgery of the digital signature*

Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature by the SVD does not detect the forgery. The signature generated by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.Expos_TOE_Disk *TOE tampering and accessing the TOE internal disk*

An attacker tampers the TOE and accesses the internal disk attempting to read the signatories' SCDs and RAD.

3.2 Organizational Security Policies

P.CSP_QCert *Qualified certificate*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (The Directive [1]: 2:9, Annex I) for the SVD generated by the SSCD or the TSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (eIDAS [18]: Annex I) for the SVD generated by the QSCD.
The certificates contains at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

P.QSign *Qualified electronic signatures*

The signatory uses a signature-creation system to sign data with an advanced electronic signature (The Directive [1]: 1, 2 or eIDAS [18]), which is a qualified electronic signature if it is based on a valid qualified certificate (Annex I on both [1] and [18]). The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD/QSCD. The SSCD/QSCD creates the digital signature created with a SCD implemented in the SSCD/QSCD that the signatory maintain under his sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

P.Sigy_SSCD_QSCD *TOE as secure signature-creation device*

The TOE meets the requirements for an SSCD/QSCD laid down in Annex III of The Directive [1] or Annex II of eIDAS [18]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD used for signature generation can practically occur only once.

P.Sig_Non-Repud *Non-repudiation of signatures*
The life cycle of the SSCD/QSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in his un-revoked certificate.

P.QTSP-ENV *QSCD is managed by a Qualified TSP*
The remote Qualified Signature Creation Device system is managed by a Qualified Trust Service Provider. The requirement is laid down in paragraph 3 of Annex II of [18].

P.QTSP-BKP *Managing backup and high availability for Disaster Recovery and business continuity purposes*
The remote Qualified Signature Creation Device solution should provide mechanisms for a secure backup and/or high availability for the purpose of Disaster Recovery and business continuity as laid down in paragraph 4 of Annex II of [18].

3.3 Assumptions

A.CGA *Trustworthy certification-generation application*

The CGA protects the authenticity of the signatory's name and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

A.SCA *Trustworthy signature-creation application*

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data the signatory wishes to sign in a form appropriate for signing by the TOE.

A.TOEConfig *TOE Configuration*

TOE configuration procedures:

- Take into account recommendation included in [6] about hash functions resistance and signature suites resistance through time,
- Give clear guidance to the appliance administrator in order to grant strict compliance to [6] in all cases it is required.
- Give clear guidance to the appliance administrator, in all cases it is required, in order to grant strict compliance to last updated version of [7] or, alternatively, in order to verify that the conditions for extended compliance to [7] are still applicable

A.SecEnv *Secure Environment*

It is assumed that the operational environment provides sufficient measures to protect the TOE against physical tampering un-authorized network access.
Also, it is assume that the operational environment provide sufficient measures to protect the TOE from using tools such as electromagnetic emanation analysis tools or dedicated sound recording tools that can try to deduce information that are used by the internal processing units of the TOE.

A.BKP-USB *Backup USB Token*

It is assumed that an authorized administrator is responsible to keep in a secure place (a safe) both backup USB tokens generated during TOE installation.

A.BKP-FILE *Backup File*

It is assumed that an authorized administrator is responsible to keep the backup file of the TOE in a secure place (a safe).

A.OTP-MGMT *OTP device and OTP device profile management*

It is assumed that OTP devices and OTP devices profiles are managed securely from the production stage (if applicable) through organizational premises until the OTP device is used by the signatory.
Also, it is assumed that the OTP devices' profiles are managed properly in the OTP Radius Server, considering also the user account status.
Remark: OTP is relevant if the TOE is installed as a Signature Creation Device.

A.NETWORK-MGMT *Routing in Secure operational environment*

It is assumed that routing infrastructure and routing administration is done in a secure manner, so that all service requests are properly sent to the Primary TOE. In the case of Primary TOE temporary fatal error, requests are assumed to be routed to a defined and selected Alternate TOE until the Primary TOE temporary fatal error is analyzed and resolved.

A.OTP-USER *OTP device usage by the signatory*

It is assumed that the signatory will keep his/her OTP device in his/her control and for any case of a missing OTP device or tampered OTP device, the signatory will report that to the organization for the purpose of revoking the signatory account and the relevant OTP device.
Remark: OTP is relevant if the TOE is installed as a Signature Creation Device.

A.Trained&Trusted *Users trained and trusted*

It is assumed that all TOE users are sufficiently trained in order to operate the TOE securely.
It is assumed in addition that TOE administrators are trusted and that they are sufficiently trained in order to install, configure the TOE and the TOE environment securely. This implies that the TOE administrators are also responsible for the secure installation, configuration and operation of the Radius Server.

Remark: In the case that the TOE is deployed as a Signature Creation Device, it is possible to configure the TOE to allow the signatory to multiply sign several documents or transactions within a fixed period of time after the two- factor authentication.
In this case, end users should be aware not to leave their application environment unattended, thus allowing other users sign on their environment

without providing their static password and OTP. In this cases it is required to close the digital signature application.

4 Security Objectives

This section identifies and defines the security objectives for the TOE and the 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.

4.1 Security Objectives for the TOE

OT.Lifecycle_Security *Lifecycle security*

The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall provide functionality to securely destroy the SCD.

Application note:
The TOE may contain more than one SCD. There is no need to destroy the SCD in case of re-generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after expiration of the (qualified) certificate for the corresponding SVD.

OT.SCD/SVD_Gen *SCD/SVD generation*

The TOE provides security features to ensure that authorized users only invoke the generation of the SCD and the SVD.

OT.SCD_Unique *Uniqueness of the signature-creation data*

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation can practically occur only once and cannot be reconstructed from the SVD. In that context ‘practically occur once’ means that the probability of equal SCDs is negligible.

OT.SCD_SVD_Corresp *Correspondence between SVD and SCD*

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating a digital signature creation with the SCD.

OT.SCD_Secrecy *Secrecy of the signature-creation data*

The secrecy of the SCD (used for signature generation) is reasonably assured against attacks with a high attack potential.

Application note:
The TOE shall keep the confidentiality of the SCD at all times in particular during SCD/SVD generation, SCD signing operation, storage and by destruction.

OT.Sig_Secure *Cryptographic security of the digital signature*

The TOE generates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD cannot be reconstructed using the digital signatures or any other data exported from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.Sigy_SigF *Signature creation function for the legitimate signatory only*

The TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others to create a digital signature. The TOE shall resist attacks with high attack potential.

OT.DTBS_Integrity_TOE *DTBS/R integrity inside the TOE*

The TOE must not alter the DTBS/R. This objective does not conflict with a signature-creation process where the TOE applies a cryptographic hash function on the DTBS/R to prepare for signature creation algorithm.

OT.Tamper_ID *Tamper detection*

The TOE provides system features that detect physical tampering of its components, and uses those features to limit security breaches.

OT.Tamper_Resistance *Tamper resistance*

The TOE prevents or resists physical tampering with specified system devices and components.

OT.Signatory_Auth *Signatory authentication based on multifactor Auth*

The TOE will strongly authenticate the signatory prior to accessing an SCD that belongs to the signatory. In the case of Signature Creation Device, the authentication will be based on presenting an Account identity as well as a Password based on a static password that is only known to the signatory as well as a dynamic password that is displayed by the OTP device of the signatory. In order to validate the OTP, the TOE will interface the OTP Radius server located in the operational environment. The Radius Server will callback the TOE for the purpose of OTP validation providing OTP device information. The TOE will use the given OTP for validation. Only after a successful presentation of an identity, static password and One-Time Password, the signatory can digitally sign. It is possible to configure the TOE to allow the user to sign several documents or transactions within a fixed period of time after a successful authentication

OT.Seal_Auth *Signatory authentication based on single factor Auth, when TOE is installed as a Seal Creation Device*

The TOE will authenticate the signatory prior to accessing an SCD that belongs to the signatory. The authentication will be based on presenting an Account identity as well as a static password that is only known to the signatory. Only after a successful presentation of an identity, static password, the signatory can digitally sign.

OT.Admin_Auth *Administrator authentication prior to any administrative operation*

The TOE will authenticate the administrator prior to any administrative operation. This excludes several operations that are performed from the TOE Web Console (in the case that TOE hardware version 8.0 is used) or the TOE's Console (in the case that TOE hardware version 7.0 is used). These operations are: Configure networking parameters of the TOE, Setting TOE current time, TOE shutdown,

Reset TOE to factory settings and viewing general parameter.
The reset tamper operation requires inserting the backup token.
All other operations (beside the viewing general parameters) requires physical access to the TOE and an operation of unplug/plug of the TOE's USB license token.
In the case of CoSign Hardware version 8.0, a all Web Console operations are carried out from a dedicated network interface.

OT.Account_Separation *Separation between different user accounts*

The TOE will make sure that user accounts are separated from each other. Users will be able to access only their own accounts and use only SCDs that belong to the specific account.
The TOE will enable several signatories to perform a digital signature operation by directing each signatory to his/her own account.
For each account the TOE maintains a list of SCDs, SVDs and graphical images. The TOE will make sure that a signatory can access only its relevant data.

OT.Account_Activation *Activating a user account only once*

The TOE will make sure that an account can be activated only by the signatory using both a static password and a dynamic password displayed by the unique OTP device of the user. During activation the user will have to set his/her static password.
If the TOE is installed as a Seal Creation Device, the activation is based on presenting an initial static password. During activation the user will have to set his/her static password.
The TOE will make sure that an already activated account cannot be activated again.
Only after a successful activation of the signatory's account, the signatory will be able to generate a SCD and get a (qualified) certificate.

OT.UserAccountDataProtection *Protecting user data when replicated*

In the case that the operational environment includes a primary TOE and one or more alternate TOEs, User Data will be periodically replicated through a secure channel from the primary TOE to the alternate TOEs. The list of alternate TOEs are managed and stored inside the primary TOE. Both confidentiality and data integrity mechanisms will be enforced to make sure that user information is concealed and not modified while transmitted between the primary TOE and its alternates TOEs.

OT.Keys&SecretData_Gen *Master keys generation and management*

During the TOE installation four Triple DES Master keys are generated by the TOE. These Master keys are kept inside the tamper device.
As part of the TOE installation, the keys are copied into two identical backup USB Smart Card token and may be used at a later stage for the event of Reset Tamper, installing an alternate appliance or restoring a primary appliance in the case of a disaster.

4.2 Security Objectives for the Operational Environment

OE.SVD_Auth *authenticity of the SVD*

The operational environment ensures the integrity of the SVD exported by the TOE to the CGA. The CGA verifies the correspondence between the SCD in the SSCD/QSCD or the Qualified electronic Seal Creation Device used by the signatory and the SVD in the input it provides to the certificate generation function of the CSP.

OE.CGA_QCert *Generation of qualified certificates*

The CGA generates a qualified certificates that includes, inter alias

- the name of the signatory controlling the TOE,
- the SVD matching the SCD stored in the TOE and controlled by the signatory,
- the advanced signature of the CSP/TSP.

The CGA confirms with the generated certificate that the SCD corresponding to the SVD is stored in a SSCD/QSCD.

OE.HID_VAD *Protection of the VAD*

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface.
In particular:
The static password of the user as well as the OTP device should be kept confidential and not disclosed to anyone beside the Signatory at any time.
For any inspected tampering to the OTP device, the signatory should report the organization that deploys the TOE.
Remark: OTP is relevant if the TOE is installed as a Signature Creation Device.

OE.DTBS_Intend *SCA sends Data intended to be signed*

The Signatory uses trustworthy SCA that

- generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,
- sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- attaches the signature produced by the TOE to the data or provides it separately.

OE.DTBS_Protect *SCA protects the data intended to be signed*

The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

OE.SecEnv *Secure Environment of the IT environment*

The operational environment shall provide sufficient measures to protect the TOE against physical tampering, un-authorized physical access or un-authorized network access.
The following procedures should be defined:

1. The TOE should be installed in a secured and controlled access area of the IT department of the organization. No one but the appliance administrator can physically access the appliance or its surroundings.
2. The TOE administrator must periodically check the appliance's case for any evidence of physical tampering. The check must be performed at least daily. Special protective screw cover "cans" are attached over two screws on the back of the appliance. These "cans" would be damaged if the appliance's case has been opened. The TOE administrator must verify that the "cans" are attached to the appliance and that they are not damaged.
3. The appliance administrator must periodically check that the secure environment of the TOE is not installed with any hardware or software that can violate the security of the TOE. This includes network sniffers and devices that may be used for timing attacks. This also include tools electromagnetic measurements tools that are aimed to deduce sensitive information emanated from the appliance. This check must be performed at least daily.
4. The two or more appliances that are used for high availability must reside in the same secured IT environment. All appliances must be inspected in the same manner as specified above.
   Also, in this case, it is required to construct a dedicated LAN. All appliances will reside in the same LAN, so that the communication between the Primary Appliance and its Alternates is not routed outside the local network.

5. When Hardware version 7.0 is used, the physical door in the front panel of the appliance should be maintained closed and locked by the physical key in the control of the appliance administrator.
6. When CoSign Hardware version 7.0 is used, some appliance administrative tasks are operated through the TOE console. The operations include general system configuration such as setting the TOE's current time and setting the TOE's networking parameters.
   These operations do not require the authentication of the appliance administrator and rely on the physical security of the environment and above physical door protection.
7. When CoSign Hardware version 8.0 is used, some appliance administrative tasks are operated through the TOE Web Console. The operations include general system configuration such as setting the TOE's current time and setting the TOE's networking parameters.
   These operations do not require the authentication of the appliance administrator and rely on the physical security of the environment.
   These operations are triggered from a Web Based console through a dedicated network interface and require physical access to the TOE and unplug/plug the license USB token.
   It is required that the network cable of the appliance administrator's PC/Laptop will be attached to the dedicated administrative network interface of the appliance before the administrative operation is started and will be detached when the administration operation is completed.
8. When the TOE is installed as a Signature Creation Device (and not as a Seal Creation Device), the operational environment includes also an OTP Radius server. The TOE access the OTP Radius server for the purpose of OTP validation, which is done as a callback to the TOE. The OTP Radius should be protected and inspected similarly to the protection and inspection of a primary or alternate TOEs.
9. When the TOE is installed as a Qualified Signature Creation Device or as a Qualified Seal Creation Device, it must be deployed and managed by a Qualified Trust Service Provider.

OE.TOEConfig *TOE Configuration according to recommendation given in [6]*

TOE Preparative Procedures shall

- Take into account recommendation included in [6] about hash function resistance and signature suites resistance through time and give to the appliance administrator clear guidelines to which hash functions and signature suites "are usable" (according to [6]) and can be configured at TOE installation time.
- Give clear guidance to the appliance administrator in order to grant strict compliance to [6] in all cases it is required.

- Give clear guidance to the appliance administrator, in all cases it is required, in order to grant strict compliance to last updated version of [7] or, alternatively, in order to verify that the conditions for extended compliance to [7] are still applicable.

OE.NETWORK-MGMT *Routing in Secure operational environment*

The operational environment shall provide sufficient measures to define a routing infrastructure and routing administration in a secure manner, so that all service requests are properly sent to the Primary TOE.
When the organization would like to handle a fast continuity of the signature service in the case of Primary TOE temporary fatal error, the routing infrastructure shall be configured to figure out that the Primary Appliance does not offer the critical service and shall be configured to forward the networking based requests to the selected Alternate TOE until the Primary TOE temporary fatal error is analyzed and resolved.
Also, the routing infrastructure shall be configured to revert to the normal operation when the Primary TOE recovered from its temporary fatal error.

OE.OTP_Devices_Profiles *Secure Management of OTP devices profiles*

In the case of a Signature Creation Device, the management of the OTP devices and OTP devices profiles will be done in a secure manner throughout the whole life-cycle of the OTP device, by procedural means outside the TOE's scope, starting from the OTP devices factory (if applicable), accepting the devices at the organization (if applicable) and uploading the devices profiles to the OTP Radius Server. The security will be maintained when assigning the OTP device or OTP device profile to a user and sending the OTP device or the OTP device profile to the user.
It should be granted that:

- It is forbidden replacing an OTP device or OTP device profile for a user after an account was activated, the user account must be revoked and a new account for the user should be created
- It is forbidden to allocate a certain user's OTP device or OTP device profile to another user
- It is forbidden to assign a specific OTP device or a specific OTP device profile to several users

The user will also need to maintain the confidentiality of the OTP device and report whenever there is any tamper to the OTP device.

OE.OTP_Radius_Server *Secure Server of the OTP devices data*

In the case of a Signature Creation Device, the TOE will interface the OTP Radius server through a Radius protocol, and provide the signatory ID along with a dummy OTP (The dummy OTP is a hash value of the real OTP and is used for completeness of the Radius Protocol, the actual validation of the OTP will be based on the OTP given by the signatory and will be performed inside the TOE). The Radius Server will callback the TOE for actual OTP validation. The OTP Radius server manages all users and all OTP devices information, which is required for the purpose of OTP validation.
The Radius Server will protect the confidentiality and integrity of the OTP Device RAD also when in transit towards the TOE.

OE.Activation_Password *Secure Management of sending activation password*

The password the user uses as part of the account activation stage will be sent by procedural means outside the TOE's scope. This will be handled by the users' administrator where the password will be sent to the user in a secure manner. There should be a strict policy that makes sure that the activation process is not exposed.

OE.Account_Activation *Account activation by signatory*

The CA will generate a certificate for the signatory only after a formal approval by the signatory that he/she committed the activation procedure, and matching the activating date of the account in audit log of the TSF.
In the case that the signatory gets a notice that his/her account was already activated, the signatory must contact the organization immediately for a suspicion that his/her account is misused.

OE.BKP-USB *Keeping the TOE Backup USB in a secure place*

Both USB tokens used to keep the 3DES Master keys generated by the TOE during the installation phase should be kept in a secure place such as a safe and should be in the responsibility of a dedicated administrative personal.
This administrative personal should not access the secured area of the TOE.
This dedicated administrative personal can access the secured area of the appliance only in the case of a recovery from a tamper event and under the authority of the appliance administrator. In this case the dedicated administrative personal will physically insert the backup USB device into the TOE as part of the *Reset Tamper* operation.
The Appliance Administrator should perform the Reset Tamper operation only if he/she is absolutely certain that the appliance was opened in a control manner.

In the case that the tamper event occurred as part of a security compromise, it is forbidden to perform the Reset Tamper operation due to the risk that bringing the appliance to a production state may compromise inner information such as the signatory's keys.

OE.BKP-FILE *Keeping the TOE Backup File in a secure place*

The secure backup of the TOE should be kept in a secure place such as a safe and should be in the responsibility of the Appliance administrator.
The Appliance Administrator should perform the backup operation routinely. This operation will keep the whole content of the appliance's database encrypted with data integrity.
In the case of a disaster, the Appliance Admin can perform a restoration operation, which is similar to an installation process.
The restoration is based is based on the given backup file and the Backup USB token.

OE.OTP-CHAR *OTP Device Characteristics*

In the case of a Signature Creation Device, the used OTP device for the purpose of signatory authentication must have the following characteristics:

- The OTP device cannot be duplicated.
- The OTP device should have tamper evidence mechanisms or tamper response mechanisms.
- Each OTP device has its unique identification or OTP device profile.

4.3 Security Objective Rationale

4.3.1 Tracing between security objectives and the security problem definition

The following table enables tracing between security objectives and the security problem definition.

Threats-Policies-Assumptions / Security objectives	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.Sig_Secure	OT.Signatory_Auth	OT.Admin_Auth	OT.Seal_Auth	OT.Account_Separation	OT.Account_Activation	OT.UserAccountDataProte	OT.Keys&SecretData_Gen	OE.CGA_QCert	OE.SVD_Auth	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.SecEnv	OE.TOEConfig	OE.NETWORK_MGMT	OE.OTP_Devices_Profiles	OE.OTP_Radius_Server	OE.Activation_Password	OE.Account_Activation	OE.BKP-USB	OE.BKP-FILE	OE.OTP-CHAR
T.Hack_Phys		X		X	X											X							X									
T.SCD_Divulg		X															X						X							X	X	
T.SCD_Derive						X				X																						
T.Sig_Forgery							X			X	X	X	X	X	X			X								X	X	X	X			
T.SVD_Forgery			X																X													
T.DTBS_Forgery									X												X	X										
T.SigF_Misuse	X							X	X		X	X	X	X	X					X	X	X				X	X	X	X			
T.Expos_TOE_DISK		X		X	X												X													X		
P.CSP_QCert	X		X															X														
P.QSign								X		X								X			X											
P.Sigy_SSCD_QSCD	X	X			X	X	X	X	X	X	X	X	X	X	X	X	X						X			X	X	X	X	X	X	X
P.Sig_Non-Repud	X	X	X	X	X		X	X	X	X	X	X	X	X	X			X	X	X	X	X				X	X	X	X			X
P. QTSP-ENV																							X									

Threats-Policies-Assumptions / Security objectives	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.Sig_Secure	OT.Signatory_Auth	OT.Admin_Auth	OT.Seal_Auth	OT.Account_Separation	OT.Account_Activation	OT.UserAccountDataProte	OT.Keys&SecretData_Gen	OE.CGA_QCert	OE.SVD_Auth	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.SecEnv	OE.TOEConfig	OE.NETWORK_MGMT	OE.OTP_Devices_Profiles	OE.OTP_Radius_Server	OE.Activation_Password	OE.Account_Activation	OE.BKP-USB	OE.BKP-FILE	OE.OTP-CHAR
P.QTSP-BKP												X					X							X								X	
A.CGA																		X	X													
A.SCA																					X											
A.SecEnv																							X									
A.TOEConfig																								X								
A.BKP-USB																														X		
A.BKP-FILE																														X	X	
A.NETWORK-MGMT																									X							
A.OTP-MGMT																										X						X
A.OTP-USER																				X						X						X
A.Trained&Trusted																							X			X	X	X	X			

Table 1 - Tracing between security objectives and security problem definition

4.3.2 Justification for the tracing

Here follows the justification for the above tracing:

4.3.2.1 OSPs and Security Objective Sufficiency

P.CSP_QCert (CSP/TSP generates qualified certificate) establishes the CSP/TSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD/QSCD under sole control of this signatory. **P.CSP_QCert** is addressed by:

- the TOE security objective **OT.Lifecycle_Security**, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage,
- the TOE security objective **OT.SCD_SVD_Corresp**, which requires the TOE to ensure the correspondence between the SVD and the SCD during their generation, and
- the security objective for the operational environment **OE.CGA_QCert** for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

P.QSign (Qualified electronic signatures) provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. **OT.Sigy_SigF** ensures signatory's sole control over the use of the SCD by requiring the TOE to provide the signature generation function for the legitimate signatory only and to protect the SCD against the use of others. **OT.Sig_Secure** ensures that the TOE generates digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. **OE.CGA_QCert** addresses the requirement of qualified or non-qualified electronic certificates building a base for the digital signature. The **OE.DTBS_Intend** ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD_QSCD (TOE as secure/qualified signature-creation device) requires the TOE to meet **Annex III** of **The Directive** [1] and **Annex II** of eIDAS [18]. This is ensured as follows:

- **OT.SCD_Unique** meets the paragraph 1(a) of **Annex** III of [1] and paragraph 1(b) of **Annex** II of [18], by the requirements that the SCD used for signature generation can practically occur only once;
- **OT.SCD_Unique**, **OT.SCD_Secrecy** and **OT.Sig_Secure** meet the requirement in paragraph 1(a) of **Annex** III of [1] and paragraph of Annex

II of [18] by the requirements to ensure secrecy of the SCD. **OT.Tamper_Resistance** address specific objectives to ensure secrecy of the SCD against specific attacks;

- **OT.SCD_Secrecy**, **OT.Sig_Secure, OT.UserAccountDataProtection, OE.SecEnv, OT.Keys&SecretData_Gen, OE.BKP-USB and OE.BKP-FILE** meet the requirement in paragraph 1(b) of **Annex** III of [1] and paragraph 1(c) of Annex II of [18] by the requirements to ensure that the SCD cannot be derived from SVD, the digital signatures or any other data exported outside the TOE. In particular:
  - **OT.UserAccountDataProtection** covers aspects related to SCD secrecy in case of SCD replication from a primary TOE to an alternate one when the TOE is configured in High Availability Configuration mode 2**,**
  - **OE.SecEnv** covers aspects related to TOE operational environment protection against physical tampering, un-authorized physical access or un-authorized network access.
  - **OT.Keys&SecretData_Gen** makes sure that key encryption keys are properly generated and kept in a secure manner.
  - **OE.BKP-USB** covers aspects related to SCD secrecy due to:
    - an accurate protection within a secure place such a safe of Triple DES Master keys used to encrypt SCDs into the TOE internal database and
    - physical access to the USB token containing the above mentioned Triple DES Master keys granted only to the Appliance Administrator in order to perform a reset tamper operation or an alternate appliance installation**.**
  - **OE.BKP-FILE** covers aspects related to SCD secrecy due to:
    - an accurate protection within a secure place such a safe of the encrypted backup file

- **OT.Sigy_SigF** meets the requirement in paragraph 1(c) of **Annex** III of [1] or Annex II of [18] by the requirements to ensure that the TOE provides the signature generation function for the legitimate signatory only and protects the SCD against the use of others;
- **OT.DTBS_Integrity_TOE** meets the requirements in paragraph 2 of Annex III of [1] and paragraph 2 of Annex II of [18] as the TOE must not alter the DTBS/R.

Paragraph 2 of Annex III of [1] and paragraph 2 of Annex II of [18**]**, requires that an SSCD/QSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send it to the SSCD/QSCD for signing.

OE.DTBS_Intend ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE.

The usage of SCD under sole control of the signatory is ensured by

- **OT.Lifecycle_Security** requiring the TOE to detect flaws during the initialisation, personalisation and operational usage,
- **OT.SCD/SVD_Gen**, which limits invoke the generation of the SCD and the SVD to authorised users only,
- **OT.Sigy_SigF**, which requires the TOE to provide the signature generation function for the legitimate signatory only and to protect the SCD against the use of others.

Also, the following measures are taken to enhance the sole control of the signatory upon the SCD:

- **OT.Admin_Auth** defines that only an administrator can initiate a signatory account and initiate an activation account for the signatory. **OT.Account_Activation** defines an activation procedure which is done by the signatory. The signatory must present the activation password as well as the unique OTP calculated by the OTP device.
- The **OE.Activation_Password** , **OE.OTP_Devices_Profiles** and **OE.OTP_Radius_Server** are aimed for the signatory to be able to uniquely perform the account activation and thus have a sole control on his/her account.
- The **OE.Account_Activation** is aimed to eliminate any above case of misusing the signatory account, thus forbidding any generation of a qualified certificate for an account that was not properly activated.
- The **OT.Signatory_Auth** and **OE.OTP_Radius_Server** mandates two factor authentication for every digital signature operation or within a certain time from authentication process.
  In the case that the TOE is deployed as a Seal device, only OT.Signatury_Auth is relevant.
- The **OE.OTP-CHAR** makes sure that only OTP devices that match the require characteristics can be used for signatory authentication.
- In the case that the TOE is installed as a Seal Creation device, **OT.Seal_Auth** require authentication prior to digital seal generation.
- The **OT.Account_Separation** eliminates the possibility of an existing signatory of the TOE using SVD of another signatory.

P.Sig_Non-Repud (*Non-repudiation of signatures***)** deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in his certificate valid at the time of signature

creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensure the aspects of signatory's sole control over and responsibility for the digital signatures generated with the TOE. **OE.CGA_QCert** ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. **OE.SVD_Auth** and **OE.CGA_QCert** require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. **OT.SCD_SVD_Corresp** ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. **OT.SCD_Unique** provides that the signatory's SCD can practically occur just once.

OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite **OE.DTBS_Intend**, **OE.DTBS_Protect** and **OT.DTBS_Integrity_TOE** ensure that the TOE generates digital signatures only for a DTBS/R that the signatory has decided to sign as DTBS. The robust cryptographic techniques required by **OT.Sig_Secure** ensure that only this SCD may generate a valid digital signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE **OT.Lifecycle_Security** (Lifecycle security), **OT.SCD_Secrecy** (Secrecy of the signature-creation data), **OT.Tamper_ID** (Tamper detection) and **OT.Tamper_Resistance** (Tamper resistance) protect the SCD against any compromise.
In addition, the signatory account lifecycle is established using **OT.Admin_Auth** , **OT.Account_Activation**, **OE.OTP_Devices_Profile, OE.OTP_Radius_Server**, **OE.Activation_Password** and **OE.Account_Activation**. Once the account is activated, **OT.Signatory_Auth, OE.OTP_Radius_Server**, **OT.Account_Separation, OE.OTP-CHAR and OE.HID_VAD,** ensures that no one but the signatory can access and use the signatory's SCD.

P.QTSP-ENV (*remote QSCD in deployed in a qualified TSP environment***)**
OE.Sec-Env ensures that the qualified TSP environment properly hosts the TOE and its whole environmental components that supports the generation of a qualified and non-qualified digital signature.

P.QTSP-BKP (*Backup and High availability support disaster recovery and business continuity***) OE.Sec-Env** ensures that the qualified TSP environment properly hosts the TOE and its whole environmental components that supports the generation of a qualified and non-qualified digital signature. It also makes sure that the TOE deployment in high availability is done correctly.
The TOE administrator can perform a backup of the primary TOE to a file. **OT.Admin-Auth** ensures that only an administrator can perform backup to the TOE. **OT.Keys&SecretData-Gen** ensures that the generated backup is secured by encryption and its integrity can be checked.

OE.BKP-FILE ensures that the backup file is kept in a secure manner.

4.3.2.2Threats and Security Objective Sufficiency

T.Hack_Phys (Physical attacks through the TOE interfaces) deals with physical attacks exploiting physical vulnerabilities of the TOE. **OT.SCD_Secrecy** preserves the secrecy of the SCD. **OT.Tamper_ID** and **OT.Tamper_Resistance** counter the threat T.Hack_Phys by detecting and by resisting tampering attacks. Also, **OE.SecEnv** will provide additional mechanisms to counter physical attacks. The **OT.UserAccountDataProtection** ensures integrity of RAD and other user data when data is replicated between the primary TOE and the alternate TOEs, any problem in the integrity of the account data, will deny usage of any SCD of the signatory's account.

T.SCD_Divulg (Storing, copying, and releasing of the signature-creation data) addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in recital (18) of **The Directive** [1],. This threat is countered by **OT.SCD_Secrecy** which assures the secrecy of the SCD used for signature creation.
OE.SecEnv ensures that the TOE is not exposed out of the secure environment of the IT department of the organization.
OT.Keys&SecretData_Gen makes sure that key encryption keys are properly generated and kept in a secure manner.
OE.BKP-USB ensures that the backup token is kept in a strict secure manner, and will be used only for dedicated purposes within the secure environment.
OE.BKP-FILE ensures that the backup file is kept in a strict secure manner, and will be used only for dedicated purposes within the secure environment.

T.SCD_Derive (Derive the signature-creation data) deals with attacks on the SCD via public known data produced by the TOE which are the SVD and the signatures created with the SCD. This threat is countered by **OT.SCD/SVD_Gen** that provides cryptographic secure generation of the SCD/SVD-pair.
OT.Sig_Secure ensures cryptographic secure digital signatures.

T.Sig_Forgery (Forgery of the digital signature) deals with non-detectable forgery of the digital signature. **OT.Sig_Secure**, **OT.SCD_Unique** and **OE.CGA_Qcert** address this threat in general. The **OT.Sig_Secure** (*Cryptographic security of the digital signature*) ensures by means of robust cryptographic techniques that the signed data and the digital signature are securely linked together. **OT.SCD_Unique** ensures that the same SCD cannot

be generated more than once and the corresponding SVD cannot be included in another certificate by chance. **OE.CGA_Qcert** prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision on a forged signature.
In the case when the TOE is deployed as a Signature Creation Device, the signatory account lifecycle is established using **OT.Admin_Auth**, **OT.Account_Activation**, **OE.OTP_Devices_Profile**, **OE.OTP_Radius_Server , OE.Activation_Password** and **OE.Account_Activation**. Once the account is activated, **OT.Signatory_Auth, OE.OTP_Radius_Server** and **OT.Account_Separation** ensures that no one but the signatory can access and use the signatory's SCD.
In the case when the TOE is deployed as a Seal Creation Device, the signatory account lifecycle is established using **OT.Admin_Auth**, **OT.Account_Activation**, **OE.Activation_Password** and **OE.Account_Activation**. Once the account is activated, **OT.Seal_Auth** and **OT.Account_Separation** ensures that no one but the signatory can access and use the signatory's SCD.

T.SVD_Forgery (*Forgery of the signature-verification data***)** deals with the forgery of the SVD exported by the TOE to the CGA to generation a certificate. T.SVD_Forgery is addressed by **OT.SCD_SVD_Corresp**, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and **OE.SVD_Auth** that ensures the integrity of the SVD exported by the TOE to the CGA.

T.DTBS_Forgery (*Forgery of the DTBS/R***)** addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of **OE.DTBS_Intend**, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of **OE.DTBS_Protect**, which ensures that the DTBS/R can not be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of **OT.DTBS_Integrity_TOE** by ensuring the integrity of the DTBS/R inside the TOE.

T.SigF_Misuse (Misuse of the signature-creation function of the TOE) addresses the threat of misuse of the TOE signature-creation function to create SDO by others than the signatory to create a digital signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c)

of Annex III of [1] and by paragraph 1(d) of Annex II of [18].
OT.Lifecycle_Security (*Lifecycle security*) requires the TOE to detect flaws during the initialisation, personalisation and operational usage including secure destruction of the SCD, which may be initiated by the signatory. **OT.Sigy_SigF** (*Signature creation function for the legitimate signatory only*) ensures that the TOE provides the signature-generation function for the legitimate signatory only. **OE.DTBS_Intend** (*Data intended to be signed*) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign and **OE.DTBS_Protect** counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. **OT.DTBS_Integrity_TOE** (*DTBS/R integrity inside the TOE*) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, **OE.HID_VAD** (*Protection of the VAD*) provides confidentiality and integrity of the VAD as needed by the authentication method employed.
When the TOE is deployed as a Signature Creation Device, the signatory account lifecycle is established using **OT.Admin_Auth**, **OT.Account_Activation**, **OE.OTP_Devices_Profile**, **OE.OTP_Radius_Server**, **OE.Activation_Password** and **OE.Account_Activation**. Once the account is activated, **OT.Signatory_Auth, OT.Seal_Auth, OE.OTP_Radius_Server** and **OT.Account_Separation** ensures that no one but the signatory can access and use the signatory's SCD.
When the TOE is deployed as a Seal Creation Device, the signatory account lifecycle is established using **OT.Admin_Auth**, **OT.Account_Activation**, **OE.Activation_Password** and **OE.Account_Activation**. Once the account is activated, **OT.Seal_Auth** and **OT.Account_Separation** ensures that no one but the signatory can access and use the signatory's SCD.

T.Expose_TOE_Disk (TOE tampering and accessing the TOE internal disk) addresses the threat of exposing the internal disk of the TOE that includes sensitive information such as the SCD of the signatories.
OT.SCD_Secrecy, OT.Keys&SecretData_Gen and **OE.BKP-USB** will eliminate the ability of an attacker to get SCD value since all signature keys are encrypted based on the value of The TOE's Critical Key 1 that is kept one Backup USB Token as well as the static password of the signatory.
OT.Tamper_ID and **OT.Tamper_Resistance** remove the Critical Keys values from any volatile and non volatile memory inside the TOE in case of tamper.

4.3.2.3 Assumptions and Security Objective Sufficiency

A.CGA (Trustworthy certification-generation application) establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is

addressed by **OE.CGA_QCert** (Generation of qualified certificates) which ensures the generation of qualified certificates and by **OE.SVD_Auth** (*Authenticity of the SVD)* which ensures the protection of the integrity and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD/QSCD.

A.SCA (Trustworthy signature-creation application) establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by **OE.DTBS_Intend** *(Data intended to be signed*) which ensures that the SCA generates the DTBS/R for the data that has been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

A.SecEnv (Secure environment) establishes sufficient measures to protect the TOE against physical tampering provided by the environment. This is addressed by **OE.SecEnv** which ensures the environment does provide the protection required.

A.TOEConfig (TOE configuration) establishes sufficient measures to grant that TOE configuration procedures takes into account recommendation included in [6] about hash functions resistance and signature suites (with reference to specific cryptographic key lengths) resistance through time. It also grants that a clear guidance will be given to the appliance administrator, in all cases it is required, in order to grant strict compliance to last updated version of [7] or, alternatively, in order to verify that the conditions for extended compliance to [7] are still applicable. This is addressed by **OE.TOEConfig** which ensures that only "usable" hash functions and signature suites as well as "usable“ algorithm to setup a secure channel between the TOE and TOE’s clients will be configured during TOE installation.

A.BKP-USB (Backup USB token) establishes sufficient measures to protect the TOE against a partial exposure of signatory SCD. This is addressed by **OE.BKP-USB** which ensures that the backup USB token cannot be used by an attacker that took control or the TOE’s internal hard disk.

A.BKP-FILE (Backup File) establishes sufficient measures to protect the TOE against a partial exposure of signatory SCD. This is addressed by **OE.BKP-File** which ensures that the backup file cannot be used by an attacker that took control or the TOE’s backup file.
Also, **OE.BKP-USB** assures that the USB token containing the master keys is not accessible for accessing secured data.

A.NETWORK-MGMT (*Routing in Secure operational environment*) establishes sufficient measures to properly handle providing service to the client in normal operation of the Primary TOE and also in the case that the Primary TOE is in temporary fatal error. This is addressed by **OE. NETWORK-MGMT** which ensures that all routing definitions are carried in secure manner, where all networking based requests from clients are routed to the Primary TOE. In the case of a Temporary fatal error to the Primary TOE, the routing infrastructure will forward the networking based requests to the selected Alternate TOE.
After the recovery of the Primary TOE, the routing infrastructure of the operational environment will revert back to sending network based requests to the primary TOE.

A.OTP-MGMT (OTP device and OTP device profile management) establishes sufficient measures to protect the TOE against unauthorized access that relates to the delivery of the OTP devices or OTP devices profiles from OTP manufacturer to the organization's IT department and the delivery of the OTP devices or OTP devices profiles from the IT department to the signatories. This is addressed by **OE.OTP_Devices_Profiles** which ensures the secure lifecycle of the OTP devices or OTP devices profiles from the manufacturing stage and until the OTP device is used by the signatory and **OE-OTP-CHAR** which ensures that the characteristics of the OTP devices are suitable for managing the OTP devices though the entire management lifecycle.

A.OTP-USER (OTP device usage by the signatory) establishes sufficient measures to protect the TOE against unauthorized access that relates to unauthorized usage of the OTP device of the signatory. **OE.OTP-CHAR** makes sure that only proper OTP devices can be used to prove the authenticity of the signatory together with a presented static password before using the SCD for digital signature operation. **OE.HID_VAD** ensures that the usage of the OTP device by the signatory does not compromise the OTP device. The signatory must maintain his/her OTP device confidential and should report to the organization for every suspected event, Also, **OE.OTP_Devices_Profiles** ensures the secure lifecycle of the OTP device and other OTP devices.

A.Trained&Trusted (Users trained and trusted) establishes sufficient measures to protect the TOE against unauthorized access of users and exploiting authentication information by administrators. This is addressed by **OE.SecEnv** which ensures the environment does provide the protection required. **OE.OTP_Devices_Profiles, OE.OTP_Radius_Server**, **OE.Activation_Password** and **OE.Account_Activation** will make sure that all necessary steps are made for enabling the signatory to maintain sole control on his/her account in the TOE.

4.4 Conclusion

All threats are countered, all OSPs are enforced and all assumptions are upheld.

5 Intentionally Left Blank

6 Security Requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE and the environment.

Security functional requirements components given in section 6.1 *security functional requirements* are drawn from Common Criteria part 2 [3]. Operations for assignment, selection, iteration and refinement have been made.

The TOE security assurance requirements statement given in section 6.2 “TOE Security Assurance Requirement” is drawn from the security assurance components from Common Criteria part 3 [4].

The following textual conventions are used in this chapter as part of every SFR:

- Iteration
  Allows a component to be used more than once with varying operations. A slash (“/”) followed by an identifier placed at the end of the component indicates an iteration.
  In the case of a reference to a iteration or a group of the same iteration, the reference will be to the group of the iterations.
  For example, iterations FDP_ACF.1.1/Activation SFP, FDP_ACF.1.2/Activation SFP,… will be referred as FDP_ACF.1/Activation SFP.
- Assignment
  Allows the specification of an identified parameter and it is represented in **bold.**
- Selection:
  Allows the specification of one or more elements from a list and it is represented in *italic*.
- Refinement:
  Allows the addition of details, that are represented in **SMALL CAPITAL BOLD**

6.1 Security Functional Requirements

6.1.1 Security Audit (FAU)

6.1.1.1Security audit data generation (FAU_GEN)

6.1.1.1.1 Audit data generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*minimum*] level of audit; and
c) [**none**].

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 (if applicable), 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, [**none**].

Application note:
Follows a table of all auditable events:

Event	Functional Component	Description
Account Creation	• FDP_ACF.1/Personalisation SFP • FCS_COP.1/AUK-ENCRYPTION • FMT_SMR.1	
Account Activation	• FDP_ACF.1/Activation SFP • FDP_ACF.1/SEAL-Activation SFP • FMT_MSA.2/Static-Password-RAD	Activation of an account. If the account is already activated the operation will result an error that will be put into the audit log.
Signing Key generation	• FCS_COP.1/SIGNING • FCS_COP.1/CORRESP • FDP_ACF.1/SCD-GEN SFP • FDP_ACF.1/SEAL-SCD-GEN SFP • FMT_MSA.1/Signatory-SCD-GEN • FMT_MSA.1/SEAL-Signatory-SCD-GEN	
Signing Key certificate	• FDP_ACF.1/Cert-IMP SFP	

Event	Functional Component	Description
Upload	• FMT_MSA.1/Signatory-CERT-IMP • FMT_MSA.2/SCD-Status • FDP_ITC.1/CERTIFICATE	
Signing Key Revocation	• FCS_CKM.4 • FDP_ACC.1/Revoke-SCD SFP • FDP_ACF.1/Revoke-SCD SFP • FDP_ACC.1/SEAL-Revoke-SCD SFP • FDP_ACF.1/SEAL-Revoke-SCD SFP • FMT_MSA.1/Signatory-SCD-DISABLE • FMT_MSA.1/SEAL-Signatory-SCD-DISABLE • FMT_MSA.2/SCD-Status • FMT_REV.1/SCD	
Digital Signature operation	• FCS_COP.1/SIGNING • FDP_ACF.1/Signature-Creation SFP • FDP_ACF.1/SEAL-Creation SFP • FMT_MSA.1/Signatory • FMT_MSA.1/SEAL-Signatory • FDP_ITC.1/DTBS • FDP_ACF.1/SVD-Transfer SFP • FDP_UIT.1/SVD-Transfer	- Generation of a certificate Request – SVD Transfer will also generate a Digital signature operation event - The operation is applicable also to an Alternate Appliance
User/Admin Change Password	• FMT_MSA.1/Signatory-Change-Password • FMT_MSA.1/Admin-Change-Password • FMT_MSA.2/Static-Password-RAD • FDP_ACC.1/Change-Password SFP • FDP_ACF.1/Change-Password SFP	
Admin Login	• FIA_UAU.1	- The operation is applicable also for an Alternate Appliance
Authentication Failures	• FIA_AFL.1 • FIA_UAU.1 • FIA_UAU.2 • FIA_UAU.5 • FTP_TRP.1	- For Appliance Administrator, the operation is also Applicable for an Alternate Appliance - For a Signatory, the operation is also Applicable for an Alternate Appliance.
User Unlock	• FDP_ACF.1/Unlock-User SFP	
User Enable	• FDP_ACF.1/Enable-User SFP	
User Disable	• FDP_ACF.1/Disable-User SFP	
User Revocation	• FMT_REV.1/User	
Installing a new alternate appliance / Changing the list of alternate appliances of a	• FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP • FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP	

Event	Functional Component	Description
primary appliance	• FMT_SMF.1	
Reset Tamper	• FMT_MOF.1	- The operation is applicable also for an Alternate Appliance
Tamper Detection	• FPT_PHP.2	- The operation is applicable also for an Alternate Appliance
Download Audit Log	• FMT_SMF.1	- The operation is applicable also for an Alternate Appliance
Upload Software Version	• FMT_SMF.1	- The operation is applicable also for an Alternate Appliance
Configure System Parameters	• FMT_SMF.1	
Uploading REST TLS Server Key	• FMT_SMF.1	- The operation is applicable also for an Alternate Appliance
Backup TOE Data	• FCS_COP.1/BKP-DATA-INTEG • FCS_COP.1/BKP-ENCRYPTION	

Table 2 - TOE Auditable events

6.1.1.1.2 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.

Application note:
FAU_GEN.2 is applicable to an Alternate Appliance in the events that are specified in Table 2.

6.1.2 Cryptographic support (FCS)

6.1.2.1Cryptographic key management (FCS_CKM)

6.1.2.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1/SIGNATURE-KEY

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA**] and specified cryptographic key sizes [**2048 and 4096 Bit**] that meet the following: [**[5], [6], and [9]**].

FCS_CKM.1.1/SYMMETRIC-KEY

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Triple-DES**] and specified cryptographic key sizes [**192 bit**] that meet the following [**[7]**].

6.1.2.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**FIPS 140-2, section 4.7.6**]

Application note:
The cryptographic key SCD will be destroyed on demand of the Signatory. The whole SCD entity will be destroyed as well. All Signatory's SCDs can be destroyed upon account revocation by the Users Administrator.

6.1.2.2Cryptographic operation (FCS_COP)

6.1.2.2.1 Cryptographic operation (FCS_COP.1)

FCS_COP.1.1/CORRESP

The TSF shall perform [**SCD/SVD correspondence verification**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**2048 bit and 4096 bit**] that meet the following: [**[5] and [6]**].

FCS_COP.1.1/SIGNING

The TSF shall perform [**digital signature-generation**]

in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**2048 bit and 4096 bit**] that meet the following: [**[5] and [6]**].

FCS_COP.1.1/DATA-INTEG

The TSF shall perform [**MAC Calculation and Verification**] in accordance with a specified cryptographic algorithm [**Triple-DES**] and cryptographic key sizes [**192 bit**] that meet the following: [**[7]**].

FCS_COP.1.1/AUK-ENCRYPTION

The TSF shall perform [**User Symmetric Key Encryption**] in accordance with a specified cryptographic algorithm [**Triple-DES**] and cryptographic key sizes [**192 bit**] that meet the following: [**[7]**].

FCS_COP.1.1/KEY-ENCRYPTION

The TSF shall perform [**Signature Key Encryption**] in accordance with a specified cryptographic algorithm [**Triple-DES**] and cryptographic key sizes [**192 bit**] that meet the following: [**[7]**].

FCS_COP.1.1/BKP-DATA-INTEG

The TSF shall perform [**MAC Calculation and Verification**] in accordance with a specified cryptographic algorithm [**Triple-DES**] and cryptographic key sizes [**192 bit**] that meet the following: [**[7]**].

FCS_COP.1.1/BKP-ENCRYPTION

The TSF shall perform [**Backup Encryption**] in accordance with a specified cryptographic algorithm [**Triple-DES**] and cryptographic key sizes [**192 bit**] that meet the following: [**[7]**].

Application note:

- Successful data integrity calculations checks, as well as key encryption/decryption operations will not be audited.
- FCS_COP.1/SIGNING SFR is also applicable for an Alternate Appliance.

6.1.3 User data protection (FDP)

6.1.3.1 Access Control Policy (FDP_ACC)

6.1.3.1.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1/Personalisation SFP	The TSF shall enforce the [**Personalization SFP**] on [**Subject = *Users Administrator*, Object = User Account, Operations = creation of user account, setting Activation password for a user account where User.Role=*Signatory***].
FDP_ACC.1.1/Activation SFP	The TSF shall enforce the [**Activation SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), Static VAD, OTP VAD, OTP Validation status, Operation = account activation**].
FDP_ACC.1.1/SEAL-Activation SFP	The TSF shall enforce the [**SEAL-Activation SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), Static VAD, Operation = account activation**].
FDP_ACC.1.1/SCD-GEN SFP	The TSF shall enforce the [**SCD-GEN SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), SCD/SVD pair, Static VAD, OTP VAD, OTP Validation status, Operation = generation of SCD/SVD pair**].

FDP_ACC.1.1/SEAL-SCD-GEN SFP	The TSF shall enforce the [**SEAL-SCD-GEN SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), SCD/SVD pair, Static VAD, Operation = generation of SCD/SVD pair**].
FDP_ACC.1.1/Cert-IMP SFP	The TSF shall enforce the [**Cert-IMP SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), SCD/SVD pair, Certificate, Operation = import of certificate**].
FDP_ACC.1.1/Signature-Creation SFP	The TSF shall enforce the [**Signature-Creation SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), SCD/SVD pair, DTBS/R sent by SCA, Static VAD, OTP VAD, OTP Validation status, Operation = digital signature**].
FDP_ACC.1.1/SEAL-Creation SFP	The TSF shall enforce the [**SEAL-Creation SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), SCD/SVD pair, DTBS/R sent by SCA, Static VAD, Operation = digital signature**].
FDP_ACC.1.1/SVD-Transfer SFP	The TSF shall enforce the [**SVD Transfer SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), SVD, Operation = export of SVD**].
FDP_ACC.1.1/Unlock-User SFP	The TSF shall enforce the [**Unlock-User SFP**] on [**Subject = *Users Administrator*, Object = User Account, Operation = Unlock user**].
FDP_ACC.1.1/Enable-User SFP	The TSF shall enforce the [**Enable-User SFP**] on [**Subject = *Users Administrator*, Object = User Account, Operation = Enable user**].

FDP_ACC.1.1/Disable-User SFP	The TSF shall enforce the [**Disable-User SFP**] on [**Subject = *Users Administrator*, Object = User Account, Operation = Disable user**].
FDP_ACC.1.1/Export-Certs SFP	The TSF shall enforce the [**Export-Certs SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), Operation = export of Certificates**].
FDP_ACC.1.1/Export-Gr-Imgs SFP	The TSF shall enforce the [**Export-Gr-Imgs SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), Operation = export of Graphical Images**].
FDP_ACC.1.1/Import-Gr-Img SFP	The TSF shall enforce the [**Import-Gr-Img SFP**] on [**Subject = *Signatory*, Object = User Account (Signatory), Operation = import of a Graphical Image**].
FDP_ACC.1.1/Revoke-User SFP	The TSF shall enforce the [**Revoke User SFP**] on [**Subject = *Users Administrator*, Object = User Account, SCDs belonging to user account (according to what stated in the table below), Operation = Revoking a user**].
FDP_ACC.1.1/Appliance-Admin SFP	The TSF shall enforce the [**Appliance-Admin SFP**] on [**Subject = *Appliance Administrator*, Object = Appliance related information, Operation = Appliance administrative operations which are not user related and not operated from the TOE's Web Console (when TOE hardware version 8.0 is used) or TOE's Console (when TOE hardware version 7.0 is used)**].

FDP_ACC.1.1/Change-Password SFP	The TSF shall enforce the [**Change-Password SFP**] on [**Subject = any user, Object = User Account, Operation = change static password**].
FDP_ACC.1.1/Revoke-SCD SFP	The TSF shall enforce the [**Revoke-SCD SFP**] on [**Subject = Signatory, Object = User Account (Signatory), SCD/SVD pair, Static VAD, OTP VAD, OTP Validation status, Operation = revoke SCD**].
FDP_ACC.1.1/SEAL-Revoke-SCD SFP	The TSF shall enforce the [**SEAL-Revoke-SCD SFP**] on [**Subject = Signatory, Object = User Account (Signatory), SCD/SVD pair, Static VAD, Operation = revoke SCD**].
FDP_ACC.1.1/BACKUP-FILE SFP	The TSF shall enforce the [**BACKUP-FILE SFP**] on [**Subject = *Appliance Administrator*, Object = Appliance related information, Operation = Backup operation**].

Application Note 1:

The following SFRs are also relevant for an Alternate Appliance: FDP_ACC.1/Signature-Creation SFP, FDP_ACC.1/SEAL-Creation SFP, FDP_ACC.1/Export-Certs SFP and FDP_ACC.1/Export-Gr-Imgs SFP

Application Note 2:

The following table summarizes the above SFPs:

ACCESS CONTROL POLICY	SUBJECT	OPERATION	OBJECT
Personalization SFP	Users administrator – S.UserAdmin with Role R.UserAdmin	Creation. Activation password is set by user administrator as part of account creation.	User Account
Activation SFP	Signatory - S.Sigy with Role R.Sigy	Account Activation	User Account where Role is R.Sigy, Static VAD, OTP VAD, OTP validation status
Seal-Activation SFP	Signatory - S.Sigy with Role R.Sigy	Account Activation	User Account where Role is R.Sigy, Static VAD
SCD-GEN SFP	Signatory - S.Sigy with Role R.Sigy	Generation of SCD/SVD pair	User Account where Role is R.Sigy, SCD/SVD pair, Static VAD, OTP VAD, OTP validation status
SEAL-SCD-GEN SFP	Signatory - S.Sigy with Role R.Sigy	Generation of SCD/SVD pair	User Account where Role is R.Sigy, SCD/SVD pair, Static VAD
Cert-IMP SFP	Signatory - S.Sigy with Role R.Sigy	Import Certificate	User Account where Role is R.Sigy, SCD/SVD pair Certificate
Signature creation SFP	Signatory - S.Sigy with Role R.Sigy	Digital Signature	User Account where Role is R.Sigy, SCD/SVD pair, DTBS/R sent by SCA, Static VAD, OTP VAD, OTP validation status

ACCESS CONTROL POLICY	SUBJECT	OPERATION	OBJECT
SEAL-Signature creation SFP	Signatory - S.Sigy with Role R.Sigy	Digital Signature	User Account where Role is R.Sigy, SCD/SVD pair, DTBS/R sent by SCA, Static VAD
SVD transfer SFP	Signatory - S.Sigy with Role With Role R.Sigy	Export of SVD	User Account where Role is R.Sigy, SVD
Unlock-user-SFP	Users administrator	Unlock user	User Account
Enable-user-SFP	Users administrator	Enable user	User Account
Disable-user-SFP	Users administrator	Disable user	User Account
Export-Certs SFP	Signatory - S.Sigy with Role R.Sigy	Export of Certificates	User Account where Role is R.Sigy
Export-GR-Imgs SFP	Signatory - S.Sigy with Role R.Sigy	Export of Graphical Images	User Account where Role is R.Sigy
Import-GR-Img SFP	Signatory - S.Sigy with Role R.Sigy	Import of a Graphical Image	User Account where Role is R.Sigy
Revoke-User SFP	Users Administrator S.UserAdmin with Role R.UserAdmin	Revoking a user	User Account, SCDs belonging to user account
Appliance-Admin SFP	Appliance Administrator S.ApplianceAdmin with Role R.ApplianceAdmin	Appliance related operations listed in FMT_SMF.1 except the Manage Users functions	Any non user related information such as the audit log or system configuration. Also all Web Console related operations are excluded - when TOE hardware version 8.0 is used. And all Console related operations are excluded - when TOE hardware version

ACCESS CONTROL POLICY	SUBJECT	OPERATION	OBJECT
			7.0 is used.
Change-Password SFP	Any Type of user	Change static password	User Account
Revoke-SCD SFP	Signatory - S.Sigy with Role R.Sigy	Revoke SCD	User Account where Role is R.Sigy, SCD/SVD pair, Static VAD, OTP VAD, OTP validation status.
SEAL-Revoke-SCD SFP	Signatory - S.Sigy with Role R.Sigy	Revoke SCD	User Account where Role is R.Sigy, SCD/SVD pair, Static VAD.
BACKUP-FILE SFP	Appliance Administrator S.ApplianceAdmin with Role R.ApplianceAdmin	Backup Appliance operation in FMT_SMF.1	Appliance's database information

Table 3 - Access control policies summary

6.1.3.2 Access Control Functions (FDP_ACF)

6.1.3.2.1 Security attribute based access control (FDP_ACF.1)

The security attributes for the user, TOE components and related status are.

User, subject or object the attribute is associated with	Attribute	Status
General Attributes of a User Account		
User account	Role	Appliance Administrator (R.ApplianceAdmin), Users Administrator (R.UserAdmin), Signatory (R.Sigy)
User account	Data integrity	yes, no
Status Attributes of a User Account		
User account	Creation status	created, not created
User account	Activation status	activated, not activated
User account	Lock status	locked, unlocked
User account	Enable status	enabled, disabled
Authentication Attributes of a User Account		
Signatory	Activation password Data	value, empty
Signatory	Static password RAD	value, empty
Signatory	OTP Device RAD (in the case of Signature Creation Device)	value, empty
Appliance Administrator, Users Administrator	Login Password Data	value, empty
Signatory	Static VAD note: The value is not kept as part of the user account. (in the case of Signature Creation Device)	value, empty
Signatory	OTP VAD note: The value is not kept as part of the user account.(in the case of Signature Creation Device)	value, empty
Signatory	OTP validation status. note: The value is calculated by the OTP validation callback (in the case of Signature Creation Device)	valid, invalid
SCD/SVD pair attributes		
SCD/SVD pair	SCD status	init, operational, not operational
SCD/SVD pair	SCD Data	value, empty
SCD/SVD pair	SVD Data	value, empty
SCD/SVD pair	Matching Certificate	certificate value

Graphical Image attributes		
Graphical Image	image	value, empty

Table 4 - Security attributes for ACFs

Personalisation SFP

FDP_ACF.1.1/Personalisation SFP

The TSF shall enforce the [**Personalisation SFP**] to objects based on the following**:** [
subject = User Account
attributes = General attributes, Status attributes and authentication attributes
and
object = User Account
attributes = General attributes and Status attributes
].

FDP_ACF.1.2/Personalisation SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(subject) User Account.Role = R.*UserAdmin* and
(object) User Account.Creation status = *not created*
and either one of the following:
1. (object) User Account.Role = R.Sigy and (object) User Account.Activation Status = *not activated* and (object) User Account.Activation Password not empty and satisfies password policy configuration
or
2. (object) User Account.Role = not *R.Sigy* and *User Account .Static Password not empty* and satisfies password policy configuration
]

FDP_ACF.1.3/Personalisation SFP

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

FDP_ACF.1.4/Personalisation SFP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**empty Activation Password**].

Application note:
The password policy configuration requires minimal password length of 6 characters.

Activation SFP

FDP_ACF.1.1/Activation SFP

The TSF shall enforce the [**Activation SFP**] to objects based on the following:[
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, Status attributes and Authentication attributes
and
object = Provided Signatory VAD
attributes = Static VAD, OTP VAD, OTP validation status
].

FDP_ACF.1.2/Activation SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User Account.Role = R.Sigy and
(Object)User_Account.Activation Status = *not activated*
and
(Object) User_Account.Activation Password *not empty*
and
(Object) Provided Static VAD not empty
and
(Object) Provided OTP VAD not empty
and
OTP validation status=valid
].

FDP_ACF.1.3/Activation SFP

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

FDP_ACF.1.4/Activation SFP

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

SEAL-Activation SFP

FDP_ACF.1.1/SEAL-Activation SFP

The TSF shall enforce the [**SEAL-Activation SFP**] to objects based on the following:[
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, Status attributes and Authentication attributes
and
object = Provided Signatory VAD
attributes = Static VAD
].

FDP_ACF.1.2/SEAL-Activation SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User Account.Role = R.Sigy and
(Object)User_Account.Activation Status = *not activated*
and
(Object) User_Account.Activation Password *not empty*
and
(Object) Provided Static VAD not empty
].

FDP_ACF.1.3/SEAL-Activation SFP

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

FDP_ACF.1.4/SEAL-Activation SFP

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

SCD-GEN SFP

FDP_ACF.1.1/SCD-GEN SFP

The TSF shall enforce the [**SCD-GEN SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and

object = User Account
attributes = General attributes, Status attributes
and
object = Provided Signatory VAD
attributes = Static VAD, OTP VAD, OTP validation status
].

FDP_ACF.1.2/SCD-GEN SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R.*Sigy* and
(Object)User Account.Activation Status = *activated*
and
(Object) Provided Static VAD not empty
and
(Object) Provided OTP VAD not empty
and
OTP validation status=valid)
].

FDP_ACF.1.3/SCD-GEN SFP

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

FDP_ACF.1.4/SCD-GEN SFP

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

SEAL-SCD-GEN SFP

FDP_ACF.1.1/SEAL-SCD-GEN SFP

The TSF shall enforce the [**SEAL-SCD-GEN SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, Status attributes
and
object = Provided Signatory VAD
attributes = Static VAD)
].

FDP_ACF.1.2/SEAL-SCD-GEN SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R.*Sigy* and
(Object)User Account.Activation Status = *activated* and
(Object) Provided Static VAD not empty
].

FDP_ACF.1.3/SEAL-SCD-GEN SFP

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

FDP_ACF.1.4/SEAL-SCD-GEN SFP

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

Cert-IMP SFP

FDP_ACF.1.1/Cert-IMP SFP

The TSF shall enforce the [**Cert-IMP SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, Status attributes and SCD/SVD pair attributes
].

FDP_ACF.1.2/Cert-IMP SFP

The TSF shall enforce the following rules to determine if an operation among controlled objects and controlled objects is allowed: [
(Subject)User_Account. Role = R.*Sigy* and
(Object)User_Account Activation Status = *activated* and
(Object)User_SCD.SCD Status = *init*
].

FDP_ACF.1.3/Cert-IMP SFP

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

FDP_ACF.1.4/Cert-IMP SFP

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

Signature-Creation SFP

FDP_ACF.1.1/Signature-Creation SFP

The TSF shall enforce the [**Signature-Creation SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes and SCD attributes
and
object = Provided Signatory VAD
attributes = Static VAD, OTP VAD, OTP validation status
].

FDP_ACF.1.2/Signature-Creation SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R.*Sigy* and
(Object)User_Account.Activation Status = *activated* and
(Object)User_Account.Account Integrity = yes and
(Object)User_Account.SCD/SVD pair.SCD status = *operational* and
(Object)User_Account.SCD/SVD pair.SCD integrity=yes and
(Object) Provided Static VAD not empty
and
(Object) Provided OTP VAD not empty
and
OTP validation status=valid]

Application note 1:

Since there can be several SCD/SVD for a certain user account, the specific identification of the SCD is provided as part of the signature creation operation

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

FDP_ACF.1.4/Signature-Creation SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

Application note 2:

The FDP_ACF.1/Signature-Creation SFP is applicable also for Alternate Appliance**.**

SEAL-Creation SFP

FDP_ACF.1.1/SEAL-Creation SFP
The TSF shall enforce the [**SEAL-Creation SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes and SCD attributes
and
object = Provided Signatory VAD
attributes = Static VAD)
].

FDP_ACF.1.2/SEAL-Creation SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R.*Sigy* and
(Object)User_Account.Activation Status = *activated* and
(Object)User_Account.Account Integrity = yes and
(Object)User_Account.SCD/SVD pair.SCD status = *operational* and
(Object)User_Account.SCD/SVD pair.SCD integrity=yes

]

Application note 1:

Since there can be several SCD/SVD for a certain user account, the specific identification of the SCD is provided as part of the signature creation operation

FDP_ACF.1.3/SEAL-Creation SFP

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

FDP_ACF.1.4/SEAL-Creation SFP

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

Application note 2:

The FDP_ACF.1/SEAL-Creation SFP is applicable also for Alternate Appliance.

SVD-Transfer SFP

FDP_ACF.1.1/SVD-Transfer SFP

The TSF shall enforce the [**SVD-Transfer SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes and SCD attributes
].

FDP_ACF.1.2/SVD-Transfer SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account. Role = R.*Sigy* and
(Object)User_Account. Activation Status = *activated*
].

FDP_ACF.1.3/SVD-Transfer SFP

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

FDP_ACF.1.4/SVD-Transfer SFP

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

Unlock-User SFP

FDP_ACF.1.1/Unlock-User SFP

The TSF shall enforce the [**Unlock-User SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes and status attributes
].

FDP_ACF.1.2/Unlock-User SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R.*UserAdmin* and
(Object)User_Account.Lock Status = *locked*
]

FDP_ACF.1.3/Unlock-User SFP

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

FDP_ACF.1.4/Unlock-User SFP

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

Enable-User SFP

FDP_ACF.1.1/Enable-User SFP

The TSF shall enforce the [**Enable-User SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes

and
object = User Account
attributes = General attributes and status attributes
].

FDP_ACF.1.2/Enable-User SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R.*UserAdmin* and
(Object)User_Account.Enable Status = *disabled*
]

FDP_ACF.1.3/Enable-User SFP

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

FDP_ACF.1.4/Enable-User SFP

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

Disable-User SFP

FDP_ACF.1.1/Disable-User SFP

The TSF shall enforce the [**Disable-User SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes and status attributes
].

FDP_ACF.1.2/Disable-User SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R.*UserAdmin* and
(Object)User_Account.Enable Status = *enabled*
]

FDP_ACF.1.3/Disable-User SFP

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

FDP_ACF.1.4/Disable-User SFP

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

Export-Certs SFP

FDP_ACF.1.1/Export-Certs SFP

The TSF shall enforce the [**Export-Certs SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes
].

FDP_ACF.1.2/Export-Certs SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R*Sigy* and
(Object)User_Account.Activation Status = *activated*
].

FDP_ACF.1.3/Export-Certs SFP

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

FDP_ACF.1.4/Export-Certs SFP

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

Application Note:

The FDP_ACF.1/Export-Gr-Imgs SFP is applicable also for an Alternate Appliance**.**

Export-Gr-Imgs SFP

FDP_ACF.1.1/Export-Gr-Imgs SFP

The TSF shall enforce the [**Export-Gr-Imgs SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes
].

FDP_ACF.1.2/Export-Gr-Imgs SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account. Role = R.*Sigy* and
(Object)User_Account.Activation Status = *activated*
].

FDP_ACF.1.3/Export-Gr-Imgs SFP

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

FDP_ACF.1.4/Export-Gr-Imgs SFP

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

Application Note:

The FDP_ACF.1/Export-Gr-Imgs SFP is applicable also for an Alternate Appliance**.**

Import-Gr-Img SFP

FDP_ACF.1.1/Import-Gr-Img SFP

The TSF shall enforce the [**Import-Gr-Img SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes
].

FDP_ACF.1.2/Import-Gr-Img SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account. Role = R.*Sigy* and
(Object)User_Account.Activation Status = *activated*
].

FDP_ACF.1.3/Import-Gr-Img SFP

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

FDP_ACF.1.4/Import-Gr-Img SFP

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

Revoke-User SFP

FDP_ACF.1.1/Revoke-User SFP

The TSF shall enforce the [**Revoke-User SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes
].

FDP_ACF.1.2/Revoke-User SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject).User_Account.Role = R.*UserAdmin*
(Object).User_Account.Role = Any
].

FDP_ACF.1.3/Revoke-User SFP

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

FDP_ACF.1.4/Revoke-User SFP

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

Appliance-Admin SFP

FDP_ACF.1.1/Appliance-Admin SFP
The TSF shall enforce the [**Appliance-Admin SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and subject=Any system information which is not user related and is not operated from the TOE's Web Console (when TOE hardware version 8.0 is used) or TOE's Console (when TOE hardware version 7.0 is used)
].

FDP_ACF.1.2/Appliance-Admin SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject).User_Account.Role = R.*ApplianceAdmin*
].

FDP_ACF.1.3/Appliance-Admin SFP
The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4/Appliance-Admin SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

Change-Password SFP

FDP_ACF.1.1/Change-Password SFP
The TSF shall enforce the [**Change-Password SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes
].

FDP_ACF.1.2/Change-Password SFP
The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
The following 2 cases are allowed:

1 - **(Subject).User_Account.Role = R.*Sigy***
and (Object).User_Account.Activation_Status = *activated*
***2* - (Subject).User_Account.Role != R.Sigy**
and (in both cases) the new password satisfies password policy configuration
].

FDP_ACF.1.3/Change-Password SFP

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

FDP_ACF.1.4/Change-Password SFP

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**empty Static Password**].

Revoke-SCD SFP

FDP_ACF.1.1/Revoke-SCD SFP

The TSF shall enforce the [**Revoke-SCD SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes and SCD attributes
and
object = Provided Signatory VAD
attributes = Static VAD, OTP VAD, OTP validation status
].

FDP_ACF.1.2/Revoke-SCD SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R.*Sigy* and
(Object)User_Account.Activation Status = *activated* and
(Object)User_Account.Account Integrity = yes and
(Object)User_Account.SCD/SVD pair.SCD status = *operational* and
(Object)User_Account.SCD/SVD pair.SCD integrity=yes and

(Object) Provided Static VAD not empty
and
(Object) Provided OTP VAD not empty
and
OTP validation status=valid
]

Application note:
Since there can be several SCD/SVD for a certain user account, the specific identification of the SCD is provided as part of the SCD revocation operation

FDP_ACF.1.3/ Revoke-SCD SFP

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

FDP_ACF.1.4/ Revoke-SCD SFP

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

SEAL-Revoke-SCD SFP

FDP_ACF.1.1/SEAL-Revoke-SCD SFP

The TSF shall enforce the [**SEAL-Revoke-SCD SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and
object = User Account
attributes = General attributes, status attributes and SCD attributes
and
object = Provided Signatory VAD
attributes = Static VAD
].

FDP_ACF.1.2/SEAL-Revoke-SCD SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject)User_Account.Role = R.*Sigy* and
(Object)User_Account.Activation Status = *activated* and

(Object)User_Account.Account Integrity = yes and
(Object)User_Account.SCD/SVD pair.SCD status = *operational* and
(Object)User_Account.SCD/SVD pair.SCD integrity=yes and
(Object) Provided Static VAD not empty
and
(Object) Provided OTP VAD not empty
and
OTP validation status=valid
]

Application note:
Since there can be several SCD/SVD for a certain user account, the specific identification of the SCD is provided as part of the SCD revocation operation

FDP_ACF.1.3/SEAL-Revoke-SCD SFP

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

FDP_ACF.1.4/SEAL-Revoke-SCD SFP

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

BACKUP-File SFP

FDP_ACF.1.1/BACKUP-File SFP

The TSF shall enforce the [**BACKUP-File SFP**] to objects based on the following: [
subject = User Account
attributes = General attributes
and subject=Any system information].

FDP_ACF.1.2/BACKUP-File SFP

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
(Subject).User_Account.Role = R.*ApplianceAdmin*
].

FDP_ACF.1.3/BACKUP-File SFP
The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4/BACKUP-File SFP
The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

6.1.3.3 Export from the TOE (FDP_ETC)

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

FDP_ETC.1.1/SVD Transfer	The TSF shall enforce the [**SVD Transfer SFP**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2/SVD Transfer	The TSF shall export the user data without the user data's associated security attributes.
FDP_ETC.1.1/Export-Certs	The TSF shall enforce the [**Export-Certs SFP**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2/Export-Certs	The TSF shall export the user data without the user data's associated security attributes.
FDP_ETC.1.1/Export-Gr-Imgs	The TSF shall enforce the [**Export-Gr-Imgs SFP**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.1.2/Export-Gr-Imgs	The TSF shall export the user data without the user data's associated security attributes.

Application notes:

- The following operations will not be audited to the audit log since they are used by the SCA upon every digital signature operation: *Export-Certs*, *Export-Gr-Imgs*.
  Also, the operation of a signatory login for the purpose of exporting certificates and graphical images or a change password operation will not be audited.
  Also, *Import-Gr-Img* operation will not be audited since it is not a valuable operation that is required to be audited.

- The FDP_ETC.1/Export-Certs and FDP_ETC.1/Export-Gr-Imgs SFRs are applicable also for an Alternate Appliance.

6.1.3.3.2 Export of user data with security attributes (FDP_ETC.2)

FDP_ETC.2.1/HA-PRI-REPL-INC-SIGKEY
The TSF shall enforce the [**HA-PRI-REPL-INC-SIGKEY SFP**] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2/HA-PRI-REPL-INC-SIGKEY
The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/HA-PRI-REPL-INC-SIGKEY
The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/HA-PRI-REPL-INC-SIGKEY
The TSF shall enforce the following rules when user data is exported from the TOE: [**The TOE is configured as HA-PRI-REPL-INC-SIGKEY**]

FDP_ETC.2.1/SEAL-HA-PRI-REPL-INC-SIGKEY
The TSF shall enforce the [**SEAL-HA-PRI-REPL-INC-SIGKEY SFP**] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2/SEAL-HA-PRI-REPL-INC-SIGKEY
The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3/SEAL-HA-PRI-REPL-INC-SIGKEY
The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4/SEAL-HA-PRI-REPL-INC-SIGKEY
The TSF shall enforce the following rules when

	user data is exported from the TOE: [**The TOE is configured as SEAL-HA-PRI-REPL-INC-SIGKEY**]

Application note:
The operation will not be audited to the audit log.

FDP_ETC.2.1/BACKUP-FILE	The TSF shall enforce the [**BACKUP-FILE SFP**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2/BACKUP-FILE	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3/BACKUP-FILE	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4/BACKUP-FILE	The TSF shall enforce the following rules when user data is exported from the TOE: [**The TOE is configured as HA-PRI-REPL-INC-SIGKEY**]
FDP_ETC.2.1/BACKUP-FILE-SEAL	The TSF shall enforce the [**BACKUP-FILE SFP**] when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2/BACKUP-FILE-SEAL	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3/BACKUP-FILE-SEAL	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4/BACKUP-FILE-SEAL	The TSF shall enforce the following rules when user data is exported from the TOE: [**The TOE is configured as SEAL-HA-PRI-REPL-INC-SIGKEY**]

6.1.3.4 Information Flow Control Policy (FDP_IFC)

The security attributes for a Primary appliance or alternate appliance are:

subject the attribute is associated with	Attribute	Status
General Attributes of a Primary Appliance		
Primary Appliance	List of Alternate Appliances	Value, empty
General Attributes of an Alternate Appliance		
Alternate Appliance	Activation status	Activated, not activated

Table 5 - Security attributes - High Availability

Remark:
An installed Alternate Appliance always receives updates from the primary appliance. To avoid receiving updates from a primary appliance, the alternate appliance must be shut down.

The security attributes for that are used by the OTP validation callback, when the TOE is deployed as a Signature Creation Device:

subject the attribute is associated with	Attribute	Status
OTP Validation callback request		
Dummy OTP	Hash value of the OTP, User ID and a Random	Value
OTP device RAD	Blob of OTP device RAD	Value

Table 6 - Security attributes - OTP Validation callback

6.1.3.4.1 Subset information Flow Control (FDP_IFC.1)

HA-PRI-REPL-INC-SIGKEY SFP

FDP_IFC.1.1/HA-PRI-REPL-INC-SIGKEY SFP

The TSF shall enforce the [**HA-PRI-REPL-INC-SIGKEY SFP**] on [**subjects= Primary CoSign Appliance and Alternate Appliance list,**
Information= Entire user account information,
Operation= User account update and sending the updates to the alternate appliances. Mode of operation allows replication of SCD data from primary Appliance to alternates
].

HA-ALT-REPL-INC-SIGKEY SFP

FDP_IFC.1.1/HA-ALT-REPL-INC-SIGKEY SFP

The TSF shall enforce the [**HA-ALT-REPL-INC-SIGKEY SFP**] on [**subjects= Alternate CoSign Appliance**
Information= Entire user account information (General attributes, Status attributes and authentication attributes of user accounts, SCD/SVD pair attributes and Graphical Image attributes)
Operation = receiving data from Primary Appliance.
].

SEAL-HA-PRI-REPL-INC-SIGKEY SFP

FDP_IFC.1.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP

The TSF shall enforce the [**SEAL-HA-PRI-REPL-INC-SIGKEY SFP**] on [**subjects= Seal Primary CoSign Appliance and Seal Alternate Appliance list,**
Information=Entire user account information,
Operation= User account update and sending the updates to the alternate appliances. Mode of operation allows replication of SCD data

from

Seal primary Appliance to alternates

].

SEAL-HA-ALT-REPL-INC-SIGKEY SFP

FDP_IFC.1.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP

The TSF shall enforce the [**SEAL-HA-ALT-REPL-INC-SIGKEY SFP**] on [**subjects= Alternate CoSign Appliance**
Information= Entire user account information (General attributes, Status attributes and authentication attributes of user accounts, SCD/SVD pair attributes and Graphical Image attributes)
Operation = receiving data from Seal Primary Appliance.
].

Application note:
The following table summarizes the above SFPs:

FLOW CONTROL POLICY	SUBJECT	INFORMATION	OPERATION
HA-PRI-REPL-INC-SIGKEY SFP	Primary CoSign Appliance and alternate appliances list	Entire user account information	Update of users accounts including SCD and graphical images information and sending the updates to the alternate appliances
HA-ALT-REPL-INC-SIGKEY SFP	Alternate CoSign Appliance	Entire User account Information	Receive data from the Primary appliance
SEAL-HA-PRI-REPL-INC-SIGKEY SFP	Seal Primary CoSign Appliance and alternate appliances list	Entire user account information	Update of users accounts including SCD and graphical images information and sending the updates to the Seal alternate appliances
SEAL-HA-ALT-REPL-INC-SIGKEY SFP	Seal Alternate CoSign Appliance	Entire User account Information	Receive data from the SealPrimary appliance

Table 7 - High Availability flow controls

OTP-VAL-CALLBACK SFP

FDP_IFC.1.1/OTP-VAL-CALLBACK SFP

> The TSF shall enforce the [**OTP-VAL-CALLBACK SFP**] on
> [**subjects = Appliance,**
> **Information = Dummy-OTP, OTP Device RAD, Internal OTP**
> **Operation = OTP validation**
>].

Application notes:

- The OTP-VAL-CALLBACK SFP is relevant when the TOE is deployed as a Signature Creation Device.
- THE OTP-VAL-CALLBACK SFP is also applicable for an Alternate Appliance.
- The following table summarizes the above SFPs:

FLOW CONTROL POLICY	SUBJECT	INFORMATION	OPERATION
OTP-VAL-CALBACK SFP	Appliance	Dummy OTP, OTP Device RAD, internal OTP	The TOE will access the internal OTP based on the given Dummy OTP and validate the internal OTP against the given OTP Device RAD.

Table 8 - OTP validation callback flow control

6.1.3.5 Information Flow Control Functions (FDP_IFF)

6.1.3.5.1 Simple Security attributes (FDP_IFF.1)

HA-PRI-REPL-INC-SIGKEY SFP

FDP_IFF.1.1/HA-PRI-REPL-INC-SIGKEY SFP

The TSF shall enforce the [**HA-PRI-REPL-INC-SIGKEY SFP**] based on the following types of subject and information security attributes: [
subject security attributes = Primary Appliance list of Alternate Appliances; Alternate Appliances status and mode of operation
Information security attributes =
Entire user Account security attributes and
security attributes include SCD data
security attributes and
graphical images security attributes
].

FDP_IFF.1.2/HA-PRI-REPL-INC-SIGKEY SFP

The TSF shall permit the information flow between a controlled subject and controlled information via a controlled operation if the following rule holds: [**User account update, SCD related update, graphic images updated**].

FDP_IFF.1.3/HA-PRI-REPL-INC-SIGKEY SFP

The TSF shall enforce the [**none**]

FDP_IFF.1.4/HA-PRI-REPL-INC-SIGKEY SFP

The TSF shall explicitly authorize an information flow based on the following rules: [**none**]

FDP_IFF.1.5/HA-PRI-REPL-INC-SIGKEY SFP

The TSF shall explicitly deny an information flow based on the following rules: [**none**]

HA-ALT-REPL-INC-SIGKEY SFP

FDP_IFF.1.1/HA-ALT-REPL-INC-SIGKEY SFP

The TSF shall enforce the [**HA-ALT-REPL –INC-SIGKEY SFP**] based on the following types of subject and information security attributes: [
subject security attributes = Alternate Appliance

Information security attributes = Entire user Account security attributes security attributes including SCD data security attributes and graphical images security attributes
].

FDP_IFF.1.2/HA-ALT-REPL-INC-SIGKEY SFP
The TSF shall permit the information flow between a controlled subject and controlled information via a controlled operation if the following rule holds: [**User account update, SCD related update, graphic images updated**].

FDP_IFF.1.3/HA-ALT-REPL-INC-SIGKEY SFP
The TSF shall enforce the [**none**]

FDP_IFF.1.4/HA-ALT-REPL-INC-SIGKEY SFP
The TSF shall explicitly authorize an information flow based on the following rules: [**none**]

FDP_IFF.1.5/HA-ALT-REPL-INC-SIGKEY SFP
The TSF shall explicitly deny an information flow based on the following rules: [**none**]

SEAL-HA-PRI-REPL-INC-SIGKEY SFP

FDP_IFF.1.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP
The TSF shall enforce the [**SEAL-HA-PRI-REPL-INC-SIGKEY SFP**] based on the following types of subject and information security attributes: [
subject security attributes = Seal Primary Appliance list of Seal Alternate Appliances; Seal Alternate Appliances status and mode of operation
Information security attributes = Entire user Account security attributes and security attributes include SCD data security attributes and graphical images security attributes
].

FDP_IFF.1.2/SEAL-HA-PRI-REPL-INC-SIGKEY SFP
The TSF shall permit the information flow between a controlled subject and controlled information via a controlled operation if the

following rule holds: [**User account update, SCD related update, graphic images updated**].

FDP_IFF.1.3/SEAL-HA-PRI-REPL-INC-SIGKEY SFP
The TSF shall enforce the [**none**]

FDP_IFF.1.4/SEAL-HA-PRI-REPL-INC-SIGKEY SFP
The TSF shall explicitly authorize an information flow based on the following rules: [**none**]

FDP_IFF.1.5/SEAL-HA-PRI-REPL-INC-SIGKEY SFP
The TSF shall explicitly deny an information flow based on the following rules: [**none**]

SEAL-HA-ALT-REPL-INC-SIGKEY SFP

FDP_IFF.1.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP
The TSF shall enforce the [**SEAL-HA-ALT-REPL –INC-SIGKEY SFP**] based on the following types of subject and information security attributes: [
subject security attributes = Seal Alternate Appliance
Information security attributes = Entire user Account security attributes security attributes
including SCD data security
attributes and graphical images
security attributes
].

FDP_IFF.1.2/SEAL-HA-ALT-REPL-INC-SIGKEY SFP
The TSF shall permit the information flow between a controlled subject and controlled information via a controlled operation if the following rule holds: [**User account update, SCD related update, graphic images updated**].

FDP_IFF.1.3/SEAL-HA-ALT-REPL-INC-SIGKEY SFP
The TSF shall enforce the [**none**]

FDP_IFF.1.4/SEAL-HA-ALT-REPL-INC-SIGKEY SFP
The TSF shall explicitly authorize an information flow based on the following rules: [**none**]

FDP_IFF.1.5/SEAL-HA-ALT-REPL-INC-SIGKEY SFP
The TSF shall explicitly deny an information flow based on the following rules: [**none**]

OTP-VAL-CALLBACK SFP

FDP_IFF.1.1/OTP-VAL-CALLBACK SFP
The TSF shall enforce the [**OTP-VAL-CALLBACK SFP**] based on the following types of subject and information security attributes: [
subject security attributes = Appliance
Information security attributes = Dummy OTP, OTP Device RAD and internal OTP].

FDP_IFF.1.2/OTP-VAL-CALLBACK SFP
The TSF shall permit the information flow between a controlled subject and controlled information via a controlled operation if the following rule holds: [**OTP validation callback**].

FDP_IFF.1.3/OTP-VAL-CALLBACK SFP
The TSF shall enforce the [**Communication from Radius Server IP only**]

FDP_IFF.1.4/OTP-VAL-CALLBACK SFP
The TSF shall explicitly authorize an information flow based on the following rules: [**none**]

FDP_IFF.1.5/OTP-VAL-CALLBACK SFP
The TSF shall explicitly deny an information flow based on the following rules: [**Any communication that is not from Radius Server IP only**]

Application note:

The OTP-VAL-CALLBACK SFP is relevant when the TOE is deployed as a Signature Creation Device.

6.1.3.6 Import from outside of the TOE (FDP_ITC)

6.1.3.6.1 Import of user data without security attributes (FDP_ITC.1)

FDP_ITC.1.1/TOE-DTBS/R
The TSF shall enforce the [**Signature-creation SFP**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/TOE-DTBS/R

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/TOE-DTBS/R

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].

FDP_ITC.1.1/TOE-DTBS/R-SEAL

The TSF shall enforce the [**SEAL-Signature-creation SFP**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/TOE-DTBS/R-SEAL

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/TOE-DTBS/R-SEAL

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].

FDP_ITC.1.1/GRIMG

The TSF shall enforce the [**Import-Gr-Img SFP**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/GRIMG

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/GRIMG

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].

FDP_ITC.1.1/CERTIFICATE

The TSF shall enforce the [**Cert-IMP SFP**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/CERTIFICATE

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3/CERTIFICATE
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**]

Application note:

The FDP_ITC.1/TOE-DTBS/R or FDP_ITC.1/TOE-DTBS/R-SEAL are applicable also to an Alternate Appliance.

6.1.3.6.2 Import of user data with security attributes (FDP_ITC.2)

FDP_ITC.2.1/HA-ALT-REPL-INC-SIGKEY
The TSF shall enforce the [**HA-ALT-REPL-INC-SIGKEY SFP**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/HA-ALT-REPL-INC-SIGKEY
The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/HA-ALT-REPL-INC-SIGKEY
The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received

FDP_ITC.2.4/HA-ALT-REPL-INC-SIGKEY
The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/HA-ALT-REPL-INC-SIGKEY
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].

FDP_ITC.2.1/SEAL-HA-ALT-REPL-INC-SIGKEY
The TSF shall enforce the [**SEAL-HA-ALT-REPL-INC-SIGKEY SFP**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/SEAL-HA-ALT-REPL-INC-SIGKEY
The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/SEAL-HA-ALT-REPL-INC-SIGKEY
The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received

FDP_ITC.2.4/SEAL-HA-ALT-REPL-INC-SIGKEY
The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/SEAL-HA-ALT-REPL-INC-SIGKEY
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].

FDP_ITC.2.1/OTP- VAL-CALLBACK
The TSF shall enforce the [**OTP-VAL-CALLBACK SFP**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/OTP- VAL-CALLBACK
The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/OTP- VAL-CALLBACK
The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received

FDP_ITC.2.4/OTP- VAL-CALLBACK
The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/OTP-VAL-CALLBACK
The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [**none**].

Application notes:

- FDP_ITC.2/HA-ALT-REPL-INC-SIGKEY and FDP_ITC.2/SEAL-HA-ALT-REPL-INC-SIGKEY related operations will not be audited to the audit log

since the source of the update in the primary appliance will be logged (for example, creation of an account).

- FDP_ITC.2/OTP-VAL-CALLBACK is relevant when the TOE is deployed as a Signature Creation Device.
- FDP_ITC.2/OTP-VAL-CALLBACK related operations will not be audited to the audit log. The whole strong authentication operation is audited as part of the Digital Signature/Activation/Key Generation operation.
- The FDP_ITC.2/OTP-VAL-CALLBACK is applicable also to an Alternate Appliance.

6.1.3.7 Stored Data Integrity (FDP_SDI)

6.1.3.7.1 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: [**User account data integrity**].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [**prohibit the use of the altered data and deny any operation upon the user account**].

Application notes:

- The user account information is described in table 4. The following information is checked for data integrity errors: General Attributes of a User Account, Status Attributes of a User Account and Authentication Attributes of a User Account beside the OTP Device RAD that is kept in the control of the Radius Server when the TOE is deployed as a Signature Creation Device.
- FDP_SDI.2 SFR is also applicable to an Alternate Appliance.

6.1.3.8 Inter-TSF user data confidentiality transfer protection (FDP_UCT)

6.1.3.8.1 Basic data exchange confidentiality (FDP_UCT.1)

FDP_UCT.1.1/HA-PRI-REPL-CONF-INC-SIGKEY
The TSF shall enforce the [**HA-PRI-REPL-INC-**

SIGKEY SFP] to [*transmit*] user data in a manner protected from unauthorized disclosure.

FDP_UCT.1.1/HA-ALT-REPL-CONF-INC-SIGKEY
The TSF shall enforce the [**HA-ALT-REPL-INC-SIGKEY SFP**] to [*receive*] user data in a manner protected from unauthorized disclosure.

FDP_UCT.1.1/SEAL-HA-PRI-REPL-CONF-INC-SIGKEY
The TSF shall enforce the [**SEAL-HA-PRI-REPL-INC-SIGKEY SFP**] to [*transmit*] user data in a manner protected from unauthorized disclosure.

FDP_UCT.1.1/SEAL-HA-ALT-REPL-CONF-INC-SIGKEY
The TSF shall enforce the [**SEAL-HA-ALT-REPL-INC-SIGKEY SFP**] to [*receive*] user data in a manner protected from unauthorized disclosure.

Application note:

Above operations will not be audited to the audit log since the source of the update in the primary appliance will be logged (for example, creation of an account).

6.1.3.9 Inter-TSF user data integrity transfer protection (FDP_UIT)

6.1.3.9.1 Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/SVD-Transfer
The TSF shall enforce the [**SVD Transfer SFP**] to [*transmit*] user data in a manner protected from [*modification*, *insertion*] errors.

FDP_UIT.1.2/SVD-Transfer
The TSF shall be able to determine on receipt of user data, whether [*modification, insertion*] has occurred.

FDP_UIT.1.1/TOE-DTBS/R
The TSF shall enforce the [**Signature-creation SFP**] to

[*receive*] user data in a manner protected from [*modification, deletion and insertion*] errors.

FDP_UIT.1.2/TOE-DTBS/R
The TSF shall be able to determine on receipt of user data, whether [*modification, deletion and insertion*] has occurred.

FDP_UIT.1.1/TOE-DTBS/R-SEAL
The TSF shall enforce the [**SEAL-Signature-creation SFP**] to [*receive*] user data in a manner protected from [*modification, deletion and insertion*] errors.

FDP_UIT.1.2/TOE-DTBS/R-SEAL
The TSF shall be able to determine on receipt of user data, whether [*modification, deletion and insertion*] has occurred.

FDP_UIT.1.1/HA-ALT-REPL-INC-SIGKEY
The TSF shall enforce the [**HA-ALT-REL-INC-SIGKEY SFP**] to be able to [*receive*] user data in a manner protected from [*modification*] errors.

FDP_UIT.1.2/HA-ALT-REPL-INC-SIGKEY
The TSF shall be able to determine on receipt of user data, whether [*modification*] has occurred.

FDP_UIT.1.1/SEAL-HA-ALT-REPL-INC-SIGKEY
The TSF shall enforce the [**SEAL-HA-ALT-REL-INC-SIGKEY SFP**] to be able to [*receive*] user data in a manner protected from [*modification*] errors.

FDP_UIT.1.2/SEAL-HA-ALT-REPL-INC-SIGKEY
The TSF shall be able to determine on receipt of user data, whether [*modification*] has occurred.

Application notes:

- FDP_UIT.1/HA-ALT-REPL-INC-SIGKEY and FDP_UIT.1/SEAL-HA-ALT-REPL-INC-SIGKEY will not be audited to the audit log since the source of the update in the primary appliance will be logged (for example, creation of an account).
- FDP_UIT.1/TOE-DTBS/R and FDP_UIT.1/TOE-DTBS/R-SEAL are also applicable to an Alternate Appliance.

6.1.4 Identification and authentication (FIA)

6.1.4.1Authentication Failure (FIA_AFL)

6.1.4.1.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within* [***3-8***]] unsuccessful authentication attempts occur related to [**consecutive failed authentication attempts**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [**lock the user account**].

Application note:

FIA_AFL.1 SFR is also applicable to an Alternate Appliance.
In the case that the user gets locked, it will not be possible to unlock the user, since the Users Administrator will not be able to perform any update on the Alternate Appliance and thus, will not be able to unlock the locked user.

6.1.4.1.2 User attribute definition (FIA_ATD)

6.1.4.1.3 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**General Attributes, Status Attributes and Authentication attributes of User account, SCD/SVD pair attributes and Graphical images attributes**].

6.1.4.2User Authentication (FIA_UAU)

6.1.4.2.1 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow **[(1) Identification of the user by means of TSF required by FIA_UID.1. (2) Establishing a trusted path between remote user and the TOE by means**

of TSF required by FTP_TRP.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.

Application note:

FIA_UAU.1 SFR is also applicable to an Alternate Appliance.

6.1.4.2.2 User Authentication Before Any Action (FIA_UAU.2)

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before any other TSF-mediated action on behalf of that user.

Application notes:

- The SFR is relevant if the TOE is deployed as a Seal Creation Device.
  As part of the authentication, any of the SCDs of the account is accessible for performing a digital signature operation.
  The encrypted SCD, as well as a special AUK is extracted from the database.
  The AUK is encrypted using a key that is built by a global master secret key and the static password of the signatory.
  The decrypted AUK is used to decrypt the encrypted SCD.
- FIA_UAU.2 SFR is also applicable to an Alternate Appliance.

6.1.4.2.3 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide [**Static user password and OTP dynamic password**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**if (Subject)User_Account.Role = R.*Sigy* multiple authentication is mandatory for a single digital signature operation or a set of digital signature operations, SCD generation and SCD revocation. For any other operation such as *change Static Password,* administrative operation, multiple authentications are not required.**
When TOE hardware version 8.0 is used - Web Console related operations authentication is not required

When TOE hardware version 7.0 is used – TOE's Console related operations authentication is not required].

Application notes:

- The SFR is relevant if the TOE is deployed as a Signature Creation Device. As part of the multi factor authentication, any of the SCDs of the account is accessible for performing a digital signature operation.
  It is possible to define a certain time period where after the authentication it will be possible to sign several digital signature operations within the same application.
  The encrypted SCD, as well as a special AUK is extracted from the database. The AUK is encrypted using a key that is built by a global master secret key and the static password of the signatory.
  The decrypted AUK is used to decrypt the encrypted SCD.
- FIA_UAU.5 SFR is also applicable to an Alternate Appliance.

6.1.4.3 User identification (FIA_UID)

6.1.4.3.1 Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**Establishing a trusted path between remote user and the TOE**] 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.

Application notes:

- Any attempt to perform a TSF related request without being authenticated previously will reject the attempt without having a dedicated entry in the audit log.
  There are some specific general commands that are identified as anonymous commands that do not require a previous user authentication.
- FIA_UID.1 SFR is also applicable to an Alternate Appliance.

6.1.5 Security management (FMT)

6.1.5.1 Management of functions in TSF (FMT_MOF)

6.1.5.1.1 Management of security functions behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [*enable*] the functions [**All functionality of the TSF**] to [**Appliance Administrator**].

Application note:

The functionality refers to the reset tamper function in the case of a temper event.

6.1.5.2 Management of security attributes (FMT_MSA)

6.1.5.2.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/Users-Administrator
The TSF shall enforce the [**Personalization SFP**] to restrict the ability to [***create***] the security attributes [**Activation Password Data**] to [**Users Administrator**].

FMT_MSA.1.1/Signatory The TSF shall enforce the [**Signature-creation SFP**] to restrict the ability to [***use to sign***] the security attributes [**SCD data**] to [**Signatory**].

FMT_MSA.1.1/SEAL-Signatory The TSF shall enforce the [**SEAL-creation SFP**] to restrict the ability to [***use to sign***] the security attributes [**SCD data**] to [**Signatory**].

FMT_MSA.1.1/Signatory-SCD-GEN
The TSF shall enforce the [**SCD-GEN SFP**] to restrict the ability to [***create***] the security attributes [**SCD data, SVD data**] to [**Signatory**].

FMT_MSA.1.1/SEAL-SignatorySCD-DISABLE
The TSF shall enforce the [SEAL-**Revoke-SCD SFP**] to restrict the ability to [*modify*] the security attributes [**SCD status**] to [**Signatory, if SCD status = *operational***].

FMT_MSA.1.1/Signatory-SEAL-SCD-NO-REVERT
The TSF shall enforce the [SEAL-**Revoke-SCD SFP**] to restrict the ability to [*modify*] the security attributes [**SCD status**] to [**nobody when SCD status = *not operational***].

FMT_MSA.1.1/Signatory-CERT-IMP
The TSF shall enforce the [**Cert-IMP SFP**] to restrict the ability to [*modify*] the security attributes [**SCD matching certificate**] to [**Signatory**].

FMT_MSA.1.1/Signatory Change Password
The TSF shall enforce the [**Change-Password SFP**] to restrict the ability to [*modify*] the security attributes [**Static Password RAD**] to [**Signatory**].

FMT_MSA.1.1/Admin-Reg Change Password
The TSF shall enforce the [**Change-Password SFP**] to restrict the ability to [*modify*] the security attributes [**Login Password Data**] to [**Users Admin, Appliance Admin**].

Application note:

FMT_MSA.1/Signatory and FMT_MSA.1/SEAL-Signatory SFRs are also applicable to an Alternate Appliance.

6.1.5.2.2 Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1/Activation-Password-Data
The TSF shall ensure that only secure values are accepted for [**Activation Password Data**].

FMT_MSA.2.1/SCD-Status
The TSF shall ensure that only secure values are accepted for [**SCD status**].

FMT_MSA.2.1/Static-Password-RAD
The TSF shall ensure that only secure values are accepted for [**Static Password RAD**].

FMT_MSA.2.1/Login-Password-Data
The TSF shall ensure that only secure values are accepted for [**Login Password Data**].

Application notes:

- FMT_MSA.2/Login-Password-Data will not be audited to the audit log in the case of a valid signatory login.
- FMT_MSA.2/Login-Password-Data is also applicable to an Alternate Appliance.

6.1.5.2.3 Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1
The TSF shall enforce the [**Personalization 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 [**users administrators**] to specify alternative initial values to override the default values when an object or information is created.

Application note:
The users administrator defines the role and either static password or activation password of the newly created user.

6.1.5.3 Revocation (FMT_REV)

6.1.5.3.1 Revocation (FMT_REV.1)

FMT_REV.1.1/SCD
The TSF shall restrict the ability to revoke [**SCD attributes**] associated with the [***Signatory***] under the control of the TSF to [**Signatory**].

FMT_REV.1.2/SCD
The TSF shall enforce the rules [**set the security attribute "SCD operational" from "yes" to "no" and destroy the SCD**].

FMT_REV.1.1/Sig-User The TSF shall restrict the ability to revoke **[status attributes**] associated with the [***any user account where User_Account.Role = R.Sigy***] under the control of the TSF to [**Users Administrator**].

FMT_REV.1.2/Sig-User The TSF shall enforce the rules [**When a Signatory user account is revoked all the associated signature keys, certificates and graphical images are deleted.**].

FMT_REV.1.1/Admin-User The TSF shall restrict the ability to revoke **[status attributes**] associated with the [***any user account where User_Account.Role <> R.Sigy***] under the control of the TSF to [**Users Administrator**].

FMT_REV.1.2/Admin-User The TSF shall enforce the rules [**When a user account is revoked all the associated information are deleted.**].

6.1.5.4 Specification of Management Function (FMT_SMF)

6.1.5.4.1 Specification of Management Functions (FMT_SMF.1)

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

- **Download Audit Log**
- **Backup Appliance information**
- **Upload a new software version. The updated software will need to be also Common Criteria certified under this Security Target or an updated version of this Security Target.**
- **Turning an Alternate appliance to a Primary appliance**
- **Installing a new alternate appliance**
- **Changing the list of alternate appliances of a primary appliance**
- **Upload REST Server TLS key**
- **Configure system parameters**
- **Manage users (create user, update user, query user's information, enable/disable a user and delete a user)**
- **Shutting down the TOE**

- **Software restart of the TOE**
- **Hardware restart of the TOE**
- **Restoring a TOE from backup using backup token and backup file**

].

Application notes:

- Download Audit Log, Upload new Software Version, Upload REST Server Key, Shutting down the TOE, Software restart of the TOE, Hardware restart of the TOE are applicable also to an Alternate Appliance as well.
- Turning an Alternate Appliance to a Primary Appliance is applicable only for an Alternate Appliance.

6.1.5.5 Security management roles (FMT_SMR)

6.1.5.5.1 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles **[Appliance Administrator (R.ApplianceAdmin), Users Administrator (R.UserAdmin), and Signatory (R.Sigy)**].

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

6.1.6 Protection of the TSF (FPT)

6.1.6.1 TSF physical protection (FPT_PHP)

6.1.6.1.1 Notifications 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 [**The entire appliance**], the TSF shall monitor the devices and elements and notify [**Appliance Administrator**] when physical tampering with the TSF's devices or TSF's elements has occurred.

Application notes:
The FPT_PHP.2 is applicable also to an Alternate Appliance.

6.1.6.1.2 Resistance to physical attack (FPT_PHP.3)

FPT_PHP.3.1 The TSF shall resist [**opening the appliance**] to the [**cover**] by responding automatically such that the SFRs are always enforced.

Application notes:
The FPT_PHP.3 is applicable also to an Alternate Appliance.

6.1.6.2Time stamps (FPT_STM)

6.1.6.2.1 Reliable time stamps (FPT_STM.1)

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

Application notes:
The FPT_STM.1 is applicable also to an Alternate Appliance.

6.1.6.3Inter-TSF TSF Data Consistency (FPT_TDC)

6.1.6.3.1 Inter-TSF basic TSF data consistency (FPT_TDC.1)

FPT_TDC.1.1/HIGH-AVAILABILITY
The TSF shall provide the capability to consistently interpret [**User Account information (including General attributes, Status attributes and authentication attributes), SCD information and graphical images**] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/HIGH-AVAILABILITY
The TSF shall use [**data integrity of the User Account information**] when interpreting the TSF data from another trusted IT product.

FPT_TDC.1.1/SEAL-HIGH-AVAILABILITY
The TSF shall provide the capability to consistently interpret [**User Account information (including General attributes, Status attributes and authentication attributes), SCD information and graphical images**] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/SEAL-HIGH-AVAILABILITY
The TSF shall use [**data integrity of the User Account information**] when interpreting the TSF data from another trusted IT product.

FPT_TDC.1.1/OTP-VAL-CALLBACK
The TSF shall provide the capability to consistently interpret [**Dummy OTP and OTP Device RAD**] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2/ OTP-VAL-CALLBACK
The TSF shall use [**data integrity of communication**] when interpreting the TSF data from another trusted IT product.

Application note:

- FPT_TDC.1/OTP-VAL-CALLBACK is relevant when the TOE is deployed as a Signature Creation Device. Also, the Radius server invokes the TOE's OTP validation callback for the purpose of validating the internal OTP using the OTP device RAD provided by the Radius Server. The interface is based on TLS secure communication, which includes data integrity mechanism.
- FPT_TDC.1/OTP-VAL-CALLBACK is applicable also to an Alternate Appliance.

6.1.6.4TSF self test (FPT_TST)

6.1.6.4.1 TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests [*during initial start-up*] 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*].

6.1.7 Trusted path/channels (FTP)

6.1.7.1 Inter-TSF trusted channel (FTP_ITC)

6.1.7.1.1 Inter-TSF trusted channel (FTP_ITC.1)

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

FTP_ITC.1.2/CoSign-Client The TSF shall permit [*another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/CoSign-Client

The TSF shall initiate communication via the trusted channel for [**all appliance management operations, user management operations**].

Application notes:
The FTP_ITC.1/CoSign-Client is also applicable to an Alternate Appliance.

FTP_ITC.1.1/PRI-APPL-INC-SIGKEY

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

FTP_ITC.1.2/PRI-APPL-INC-SIGKEY

The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3/PRI-APPL-INC-SIGKEY

The TSF shall initiate communication via the trusted channel for [**updating user information in the alternate appliance**].

FTP_ITC.1.1/ALT-APPL-INC-SIGKEY

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

FTP_ITC.1.2/ALT-APPL-INC-SIGKEY

The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3/ALT-APPL-INC-SIGKEY

The TSF shall initiate communication via the trusted channel for [**receiving data from Primary Appliance**].

FTP_ITC.1.1/SEAL-PRI-APPL-INC-SIGKEY

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

FTP_ITC.1.2/SEAL-PRI-APPL-INC-SIGKEY

The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3/SEAL-PRI-APPL-INC-SIGKEY

The TSF shall initiate communication via the trusted channel for [**updating user information in the alternate appliance**].

FTP_ITC.1.1/SEAL-ALT-APPL-INC-SIGKEY

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

FTP_ITC.1.2/SEAL-ALT-APPL-INC-SIGKEY

The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3/SEAL-ALT-APPL-INC-SIGKEY

The TSF shall initiate communication via the trusted channel for [**receiving data from Primary Appliance**].

FTP_ITC.1.1/Radius-Server

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

FTP_ITC.1.2/Radius-Server

The TSF shall permit [*another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3/Radius-Server	The TSF shall initiate communication via the trusted channel for [**OTP Validation callback**].

Application notes:

- Above will not be audited to the audit log since the source of the update in the primary appliance will be logged (for example, creation of an account).
- FTP_ITC.1/Radius-Server is relevant when the TOE is deployed as a Signature Creation Device. Also, it will restrict communication only from the Radius Server based on the Radius Server's IP address.
- FTP_ITC.1/Radius-Server SFR is also applicable to an Alternate Appliance.

6.1.7.2Trusted path (FTP_TRP)

6.1.7.2.1 Trusted path (FTP_TRP.1)

FTP_TRP.1.1	The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification or disclosure*].
FTP_TRP.1.2	The TSF shall permit [*remote 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,*[**user sessions**]].

Application note:

FTP_TRP.1 SFR is also applicable to an Alternate Appliance.

6.2 Security Assurance Requirements

The assurance level for this TOE is EAL4+ AVA_VAN.5, ALC_FLR.1, ATE_DPT.2.

Assurance Class	Assurance components
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 - ALC_FLR.1 Basic flaw remediation
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.2 Testing: security enforcing modules - ATE_IND.2 Independent testing – sample - ATE_FUN.1 Functional testing
AVA: Vulnerability assessment	- AVA_VAN.5 Advanced methodical vulnerability analysis

Table 9 - Assurance Requirements: EAL4+ AVA_VAN.5, ALC_FLR.1, ATE_DPT.2

Follows a SFR dependency satisfaction table

Requirement	Dependencies
FAU_GEN.1	- FPT_STM.1
FAU_GEN.2	- FAU_GEN.1 - FIA_UID.1
FCS_CKM.1/SIGNATURE-KEY	- FCS_COP.1/CORRESP - FCS_COP.1/SIGNING - FCS_CKM.4
FCS_CKM.1/SYMMETRIC-KEY	- FCS_COP.1/DATA-INTEG - FCS_COP.1/AUK-ENCRYPTION - FCS_COP.1/BKP-DATA-INTEG - FCS_COP.1/BKP-ENCRYPTION - FCS_CKM.4
FCS_CKM.4	- FCS_CKM.1 - FDP_ITC.2/HA-ALT-REPL-INC-SIGKEY - FDP_ITC.2/SEAL-HA-ALT-REPL-INC-SIGKEY
FCS_COP.1/CORRESP	- FCS_CKM.1/SIGNATURE-KEY - FCS_CKM.4
FCS_COP.1/SIGNING	- FCS_CKM.1/SIGNATURE-KEY - FCS_CKM.4
FCS_COP.1/DATA-INTEG	- FCS_CKM.1/SYMMETRIC-KEY - FCS_CKM.4
FCS_COP.1/AUK-ENCRYPTION	- FCS_CKM.1/SYMMETRIC-KEY - FCS_CKM.4
FCS_COP.1/KEY-ENCRYPTION	- FCS_CKM.1/SYMMETRIC-KEY - FCS_CKM.4
FCS_COP.1/BKP-DATA-INTEGRITY	- FCS_CKM.1/SYMMETRIC-KEY - FCS_CKM.4
FCS_COP.1/BKP-ENCRYPTION	- FCS_CKM.1/SYMMETRIC-KEY - FCS_CKM.4
FDP_ACC.1/Personalisation SFP	- FDP_ACF.1/Personalisation SFP
FDP_ACC.1/Activation SFP	- FDP_ACF.1/Activation SFP
FDP_ACC.1/SEAL-Activation SFP	- FDP_ACF.1/SEAL-Activation SFP
FDP_ACC.1/SCD-GEN SFP	- FDP_ACF.1/SCD-GEN SFP
FDP_ACC.1/SEAL-SCD-GEN SFP	- FDP_ACF.1/SEAL-SCD-GEN SFP
FDP_ACC.1/Cert-IMP SFP	- FDP_ACF.1/Cert-IMP SFP
FDP_ACC.1/Signature-Creation SFP	- FDP_ACF.1/Signature-Creation SFP
FDP_ACC.1/SEAL-Creation SFP	- FDP_ACF.1/SEAL-Creation SFP
FDP_ACC.1/SVD-Transfer SFP	- FDP_ACF.1/SVD-Transfer SFP
FDP_ACC.1/Unlock-User SFP	- FDP_ACF.1/Unlock-User SFP
FDP_ACC.1/Enable-User SFP	- FDP_ACF.1/Enable-User SFP
FDP_ACC.1/Disable-User SFP	- FDP_ACF.1/Disable-User SFP
FDP_ACC.1/Export-Certs SFP	- FDP_ACF.1/Export-Certs SFP

Requirement	Dependencies
FDP_ACC.1/Export-Gr-Imgs SFP	- FDP_ACF.1/Export-Gr-Imgs SFP
FDP_ACC.1/Import-Gr-Img SFP	- FDP_ACF.1/Import-Gr-Img SFP
FDP_ACC.1/Revoke-User SFP	- FDP_ACF.1/Revoke-User SFP
FDP_ACC.1/Appliance-Admin SFP	- FDP_ACF.1/Appliance-Admin SFP
FDP_ACC.1/Change-Password SFP	- FDP_ACF.1/Change-Password SFP
FDP_ACC.1/Revoke-SCD SFP	- FDP_ACF.1/Revoke-SCD SFP
FDP_ACC.1/SEAL-Revoke-SCD SFP	- FDP_ACF.1/SEAL-Revoke-SCD SFP
FDP_ACF.1/Personalisation SFP	- FDP_ACC.1/Personalisation - FMT_MSA.3
FDP_ACF.1/Activation SFP	- FDP_ACC.1/Activation - FMT_MSA.3
FDP_ACF.1/SEAL-Activation SFP	- FDP_ACC.1/SEAL-Activation - FMT_MSA.3
FDP_ACF.1/SCD-GEN SFP	- FDP_ACC.1/SCD-GEN - FMT_MSA.3
FDP_ACF.1/SEAL-SCD-GEN SFP	- FDP_ACC.1/SEAL-SCD-GEN - FMT_MSA.3
FDP_ACF.1/Cert-IMP SFP	- FDP_ACC.1/Cert-IMP - FMT_MSA.3
FDP_ACF.1/Signature-Creation SFP	- FDP_ACC.1/Signature-Creation - FMT_MSA.3
FDP_ACF.1/SEAL-Creation SFP	- FDP_ACC.1/SEAL-Creation - FMT_MSA.3
FDP_ACF.1/SVD-Transfer SFP	- FDP_ACC.1/SVD-Transfer - FMT_MSA.3
FDP_ACF.1/Unlock-User SFP	- FDP_ACC.1/Unlock-User SFP - FMT_MSA.3
FDP_ACF.1/Enable-User SFP	- FDP_ACC.1/Enable-User SFP - FMT_MSA.3
FDP_ACF.1/Disable-User SFP	- FDP_ACC.1/Disable-User SFP - FMT_MSA.3
FDP_ACF.1/Export-Certs SFP	- FDP_ACC.1/Export-Certs SFP - FMT_MSA.3
FDP_ACF.1/Export-Gr-Imgs SFP	- FDP_ACC.1/Export-Gr-Imgs SFP - FMT_MSA.3
FDP_ACF.1/Import-Gr-Img SFP	- FDP_ACC.1/Import-Gr-Img SFP - FMT_MSA.3
FDP_ACF.1/Revoke-User SFP	- FDP_ACC.1/Revoke-User SFP - FMT_MSA.3
FDP_ACF.1/Appliance-Admin SFP	- FDP_ACC.1/Appliance-Admin SFP - FMT_MSA.3
FDP_ACF.1/Change-Password SFP	- FDP_ACC.1/Change-Password SFP - FMT_MSA.3
FDP_ACF.1/Revoke-SCD SFP	- FDP_ACC.1/Revoke-SCD SFP

Requirement	Dependencies
	- FMT_MSA.3
FDP_ACF.1/SEAL-Revoke-SCD SFP	- FDP_ACC.1/SEAL-Revoke-SCD SFP - FMT_MSA.3
FDP_ETC.1/SVD Transfer	- FDP_ACC.1/SVD-Transfer SFP
FDP_ETC.1/Export-Certs	- FDP_ACC.1/Export-Certs SFP
FDP_ETC.1/Export-Gr-Imgs	- FDP_ACC.1/Export-Gr-Imgs SFP
FDP_ETC.2/HA-PRI-REPL-INC-SIGKEY	- FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP
FDP_ETC.2/SEAL-HA-PRI-REPL-INC-SIGKEY	- FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP
FDP_ETC.2/BACKUP-FILE	- FDP_ACC.1/BACKUP-FILE
FDP_ETC.2/BACKUP-FILE-SEAL	- FDP_ACC.1/BACKUP-FILE
FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP	- FDP_IFF.1/HA-PRI-REPL-INC-SIGKEY SFP
FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP	- FDP_IFF.1/HA-ALT-REPL-INC-SIGKEY SFP
FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP	- FDP_IFF.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP
FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP	- FDP_IFF.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP
FDP_IFC.1/OTP-VAL-CALLBACK SFP	- FDP_IFF.1/OTP-VAL-CALLBACK SFP
FDP_IFF.1/HA-PRI-REPL-INC-SIGKEY SFP	- FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP - FMT_MSA.3
FDP_IFF.1/HA-ALT-REPL-INC-SIGKEY SFP	- FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP - FMT_MSA.3
FDP_IFF.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP	- FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP - FMT_MSA.3
FDP_IFF.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP	- FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP - FMT_MSA.3
FDP_IFF.1/OTP-VAL-CALLBACK SFP	- FDP_IFC.1/OTP-VAL-CALLBACK SFP - FMT_MSA.3
FDP_ITC.1/TOE-DTBS/R	- FDP_ACC.1/Signature-Creation SFP - FMT_MSA.3
FDP_ITC.1/TOE-DTBS/R-SEAL	- FDP_ACC.1/SEAL-Creation SFP - FMT_MSA.3
FDP_ITC.1/GRIMG	- FDP_ACC.1/Import-Gr-Img SFP - FMT_MSA.3
FDP_ITC.1/CERTIFICATE	- FDP_ACC.1/Cert-IMP SFP - FMT_MSA.3
FDP_ITC.2/HA-ALT-REPL-INC-SIGKEY	- FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP - FTP_ITC.1/ALT-APPL-INC-SIGKEY

Requirement	Dependencies
	- FPT_TDC.1/HIGH-AVAILABILITY
FDP_ITC.2/SEAL-HA-ALT-REPL-INC-SIGKEY	- FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP - FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY - FPT_TDC.1/SEAL-HIGH-AVAILABILITY
FDP_ITC.2/ OTP-VAL-CALLBACK	- FDP_IFC.1/OTP-VAL-CALLBACK SFP - FTP_ITC.1/Radius-Server - FPT_TDC.1/OTP-VAL-CALLBACK
FDP_SDI.2	-
FDP_UCT.1/HA-PRI-REPL-CONF-INC-SIGKEY	- FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP - FTP_ITC.1/PRI-APPL-INC-SIGKEY - FTP_ITC.1/ALT-APPL-INC-SIGKEY
FDP_UCT.1/HA-ALT-REPL-CONF-INC-SIGKEY	- FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP - FTP_ITC.1/PRI-APPL-INC-SIGKEY - FTP_ITC.1/ALT-APPL-INC-SIGKEY
FDP_UCT.1/SEAL-HA-PRI-REPL-CONF-INC-SIGKEY	- FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP - FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY - FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY
FDP_UCT.1/ SEAL-HA-ALT-REPL-CONF-INC-SIGKEY	- FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP - FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY - FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY
FDP_UIT.1/SVD-Transfer	- FDP_ACC.1/SVD-Transfer SFP - FTP_ITC.1/CoSign-Client
FDP_UIT.1/TOE-DTBS/R	- FDP_ACC.1/Signature-Creation SFP - FTP_ITC.1/CoSign Client
FDP_UIT.1/TOE-DTBS/R-SEAL	- FDP_ACC.1/SEAL-Creation SFP - FTP_ITC.1/CoSign Client
FDP_UIT.1/HA-ALT-REPL-INC-SIGKEY	- FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP - FTP_ITC.1/ALT-APPL-INC-SIGKEY
FDP_UIT.1/SEAL-HA-ALT-REPL-INC-SIGKEY	- FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP - FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY
FIA_AFL.1	- FIA_UAU.1
FIA_ATD.1	-
FIA_UAU.1	- FIA_UID.1
FIA_UAU.2	- FIA_UID.1
FIA_UAU.5	-
FIA_UID.1	-
FMT_MOF.1	- FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/Users-Administrator	- FDP_ACC.1/Personalisation SFP - FMT_SMR.1

Requirement	Dependencies
	- FMT_SMF.1
FMT_MSA.1/Signatory	- FDP_ACC.1/Signature-Creation SFP - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/SEAL-Signatory	- FDP_ACC.1/SEAL-Creation SFP - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/Signatory-SCD-GEN	- FDP_ACC.1/SCD-GEN SFP - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/SEAL-Signatory-SCD-GEN	- FDP_ACC.1/SEAL-SCD-GEN SFP - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/Signatory-SCD-DISABLE	- FDP_ACC.1/Revoke-SCD SFP - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/SEAL-Signatory-SCD-DISABLE	- FDP_ACC.1/SEAL-Revoke-SCD SFP - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/Signatory-SCD-NO-REVERT	- FDP_ACC.1/Revoke-SCD SFP - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/SEAL-Signatory-SCD-NO-REVERT	- FDP_ACC.1/SEAL-Revoke-SCD SFP - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/Signatory-CERT-IMP	- FDP_ACC.1/Cert-IMP SFP - FMT_SMR.1 - FMT_SMF.1
FMT_MSA.1/Signatory-Change Password	- FMT_SMR.1 - FMT_SMF.1 - FDP_ACC.1/Change-Password SFP
FMT_MSA.1/Admin-Change-Password	- FMT_SMR.1 - FMT_SMF.1 - FDP_ACC.1/Change-Password SFP
FMT_MSA.2/Activation-Password-Data	- FDP_ACC.1/Personalisation SFP - FDP_ACC.1/Activation SFP - FDP_ACC.1/SEAL-Activation SFP - FMT_MSA.1/Users-Administrator - FMT_SMR.1
FMT_MSA.2/SCD-Status	- FDP_ACC.1/SCD-GEN SFP - FDP_ACC.1/SEAL-SCD-GEN SFP - FDP_ACC.1/Cert-IMP SFP - FMT_MSA.1/Signatory-SCD-GEN - FMT_MSA.1/Signatory-SCD-DISABLE

Requirement	Dependencies
	- FMT_MSA.1/Signatory-SCD-NO-REVERT - FMT_MSA.1/SEAL-Signatory-SCD-GEN - FMT_MSA.1/SEAL-Signatory-SCD-DISABLE - FMT_MSA.1/SEAL-Signatory-SCD-NO-REVERT - FMT_SMR.1
FMT_MSA.2/Static-Password-RAD	- FDP_ACC.1/Activation SFP - FDP_ACC.1/SEAL-Activation SFP - FDP_ACC.1/Change-Password SFP - FMT_MSA.1/Signatory-Change-Password - FMT_SMR.1
FMT_MSA.2/Login-Password-Data	- FDP_ACC.1/Personalisation SFP - FDP_ACC.1/Change-Password SFP - FMT_MSA.1/Admin-Change-Password - FMT_SMR.1
FMT_MSA.3	- FMT_MSA.1/Users-Administrator - FMT_SMR.1
FMT_REV.1/SCD	- FMT_SMR.1
FMT_REV.1/User	- FMT_SMR.1
FMT_SMF.1	-
FMT_SMR.1	- FIA_UID.1
FPT_PHP.2	- FMT_MOF.1
FPT_PHP.3	-
FPT_STM.1	-
FPT_TDC.1/HIGH-AVAILABILITY	-
FPT_TDC.1/SEAL-HIGH-AVAILABILITY	-
FPT_TDC.1/OTP-VAL-CALLBACK	-
FPT_TST.1	-
FTP_ITC.1/CoSign-Client	-
FTP_ITC.1/PRI-APPL-INC-SIGKEY	-
FTP_ITC.1/ALT-APPL-INC-SIGKEY	-
FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY	-
FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY	-
FTP_ITC.1/Radius-Server	-
FTP_TRP.1	-

Table 10 - SFR dependency satisfaction table

6.3 Security Requirements Rationale

6.3.1 Security Requirements Coverage

The following table provides a tracing between the Security Functional Requirements and the security objectives for the TOE.

TOE SFR / TOE Security Objectives	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.Signatory_Auth	OT.AdminAuth	OT.Seal_Auth	OT.Account_Separation	OT.Account_Activation	OT.UserAccountDataProtec	OT.Keys&SecretData_Gen
FAU_GEN.1	X																
FAU_GEN.2	X																
FCS_CKM.1/SIGNATURE-KEY	X	X	X				X										
FCS_CKM.1/SYMMETRIC-KEY		X									X		X	X			X
FCS_CKM.4	X	X															
FCS_COP.1/CORRESP			X														
FCS_COP.1/SIGNING										X							
FCS_COP.1/DATA-INTEG																X	
FCS_COP.1/AUK-ENCRYPTION		X															
FCS_COP.1/KEY-ENCRYPTION		X												X			
FCS_COP.1/BKP-DATA-INTEG																	
FCS_COP.1/BKP-ENCRYPTION																	
FDP_ACC.1/Personalisation SFP	X					X			X					X			
FDP_ACC.1/Activation SFP	X					X			X					X	X		
FDP_ACC.1/SEAl-Activation SFP	X					X			X					X	X		
FDP_ACC.1/SCD-GEN SFP	X	X				X			X					X			
FDP_ACC.1/SEAL-SCD-GEN SFP	X	X				X			X					X			
FDP_ACC.1/Cert-IMP SFP	X					X			X					X			
FDP_ACC.1/Signature-Creation SFP	X							X	X	X				X			
FDP_ACC.1/SEAL-Creation SFP	X							X	X	X				X			
FDP_ACC.1/SVD-Transfer SFP	X					X			X					X			
FDP_ACC.1/Unlock-User SFP	X													X			
FDP_ACC.1/Enable-User SFP	X													X			
FDP_ACC.1/DIsable-User SFP	X													X			
FDP_ACC.1/Export-Certs SFP														X			
FDP_ACC.1/Export-Gr-Imgs SFP														X			
FDP_ACC.1/Import-Gr-Img SFP														X			

TOE SFR / TOE Security Objectives	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.Signatory_Auth	OT.AdminAuth	OT.Seal_Auth	OT.Account_Separation	OT.Account_Activation	OT.UserAccountDataProtec	OT.Keys&SecretData_Gen
FDP_ACC.1/Revoke-User SFP	X													X			
FDP_ACC.1/Appliance-Admin SFP						X								X			
FDP_ACC.1/Change-Password SFP											X	X	X				
FDP_ACC.1/Revoke-SCD SFP	X	X							X					X			
FDP_ACC.1/SEAL-Revoke-SCD SFP	X	X							X					X			
FDP_ACC.1/BACKUP-FILE SFP																	
FDP_ACF.1/Personalisation SFP	X					X			X					X			
FDP_ACF.1/Activation SFP	X					X			X					X	X		
FDP_ACF.1/SEAL-Activation SFP	X					X			X					X	X		
FDP_ACF.1/SCD-GEN SFP	X	X				X			X					X			
FDP_ACF.1/SEAL-SCD-GEN SFP	X	X				X			X					X			
FDP_ACF.1/Cert-IMP SFP	X								X					X			
FDP_ACF.1/Signature-Creation SFP	X							X	X	X				X			
FDP_ACF.1/SEAL-Creation SFP	X							X	X	X				X			
FDP_ACF.1/SVD-Transfer SFP	X								X					X			
FDP_ACF.1/Unlock-User SFP	X													X			
FDP_ACF.1/Enable-User SFP	X													X			
FDP_ACF.1/Disable-User SFP	X													X			
FDP_ACF.1/Export-Certs SFP														X			
FDP_ACF.1/Export-Gr-Imgs SFP														X			
FDP_ACF.1/Import-Gr-Img SFP														X			
FDP_ACF.1/Revoke-User SFP	X													X			
FDP_ACF.1/Appliance-Admin SFP												X					
FDP_ACF.1/Change-Password SFP											X	X	X				
FDP_ACF.1/Revoke-SCD SFP	X	X							X					X			
FDP_ACF.1/SEAL-Revoke-SCD SFP	X	X							X					X			
FDP_ACF.1/BACKUP-FILE SFP																	
FDP_ETC.1/SVD Transfer SFP														X			
FDP_ETC.1/Export-Certs														X			
FDP_ETC.1/Export-Gr-Imgs														X			
FDP_ETC.2/HA-PRI-REPL-INC-SIGKEY		X	X						X	X						X	
FDP_ETC.2/SEAL-HA-PRI-REPL-INC-SIGKEY		X	X						X	X						X	
FDP_ETC.2/BACKUP-FILE																	
FDP_ETC.2/BACKUP-FILE-SEAL																	
FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP		X	X						X	X						X	
FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP		X	X						X	X						X	
FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP		X	X						X	X						X	
FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP		X	X						X	X						X	
FDP_IFC.1/OTP-VAL-CALLBACK SFP											X						
FDP_IFF.1/HA-PRI-REPL-INC-SIGKEY SFP		X	X						X	X						X	
FDP_IFF.1/HA-ALT-REPL-INC-SIGKEY SFP		X	X						X	X						X	

TOE SFR / TOE Security Objectives	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.Signatory_Auth	OT.AdminAuth	OT.Seal_Auth	OT.Account_Separation	OT.Account_Activation	OT.UserAccountDataProtec	OT.Keys&SecretData_Gen
FDP_IFF.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP		X	X						X	X						X	
FDP_IFF.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP		X	X						X	X						X	
FDP_IFF.1/OTP-VAL-CALLBACK											X						
FDP_ITC.1/TOE-DTBS/R								X						X			
FDP_ITC.1/TOE-DTBS/R-SEAL								X						X			
FDP_ITC.1/GRIMG														X			
FDP_ITC.1/CERTIFICATE														X			
FDP_ITC.2/HA-ALT-REPL-INC-SIGKEY		X	X						X	X						X	
FDP_ITC.2/SEAL-HA-ALT-REPL-INC-SIGKEY		X	X						X	X						X	
FDP_SDI.2		X	X						X	X						X	
FDP_UCT.1/HA-PRI-REPL-CONF-INC-SIGKEY		X	X						X	X						X	
FDP_UCT.1/HA-ALT-REPL-CONF-INC-SIGKEY		X	X						X	X						X	
FDP_UCT.1/ SEAL-HA-PRI-REPL-CONF-INC-SIGKEY		X	X						X	X						X	
FDP_UCT.1/ SEAL-HA-ALT-REPL-CONF-INC-SIGKEY		X	X						X	X						X	
FDP_UIT.1/SVD-Transfer														X			
FDP_UIT.1/TOE-DTBS/R								X						X			
FDP_UIT.1/TOE-DTBS/R-SEAL								X						X			
FDP_UIT.1/HA-ALT-REPL-INC-SIGKEY		X	X						X	X						X	
FDP_UIT.1/SEAL-HA-ALT-REPL-INC-SIGKEY		X	X						X	X						X	
FIA_AFL.1						X			X					X			
FIA_ATD.1						X			X					X			
FIA_UAU.1						X						X	X	X			
FIA_UAU.2		X				X			X		X			X			
FIA_UAU.5		X				X			X		X			X			
FIA_UID.1						X			X		X	X	X	X			
FMT_MOF.1	X	X							X					X			
FMT_MSA.1/Users-Administrator	X					X								X			
FMT_MSA.1/Signatory	X								X					X			
FMT_MSA.1/Signatory-SCD-GEN	X	X							X					X			
FMT_MSA.1/Signatory-SCD-DISABLE	X	X							X					X			
FMT_MSA.1/Signatory-SCD-NO-REVERT	X	X							X					X			
FMT_MSA.1/SEAL-Signatory-SCD-GEN	X	X							X					X			
FMT_MSA.1/SEAL-Signatory-SCD-DISABLE	X	X							X					X			
FMT_MSA.1/SEAL-Signatory-SCD-NO-REVERT	X	X							X					X			
FMT_MSA.1/Signatory-CERT-IMP	X								X					X			

TOE SFR / TOE Security Objectives	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Gen	OT.SCD_Unique	OT.DTBS_Integrity_TOE	OT.Sigy_SigF	OT.Sig_Secure	OT.Signatory_Auth	OT.AdminAuth	OT.Seal_Auth	OT.Account_Separation	OT.Account_Activation	OT.UserAccountDataProtec	OT.Keys&SecretData_Gen
FMT_MSA.1/Signatory-Change- Password		X				X								X			
FMT_MSA.1/Admin-Change-Password														X			
FMT_MSA.2/Activation-Password-Data	X					X								X	X		
FMT_MSA.2/SCD-Status	X	X												X			
FMT_MSA.2/Static-Password-RAD	X					X								X			
FMT_MSA.2/Login-Password-Data	X					X								X			
FMT_MSA.3	X													X			
FMT_REV.1/SCD	X	X															
FMT_REV.1/User	X																
FMT_SMF.1	X													X			
FMT_SMR.1	X	X							X					X			
FPT_PHP.2				X													X
FPT_PHP.3		X			X												X
FPT_STM.1	X																
FPT_TDC.1/HIGH-AVAILABILITY		X	X						X	X						X	
FPT_TDC.1/SEAL-HIGH-AVAILABILITY		X	X						X	X						X	
FPT_TDC.1/OTP-VAL-CALLBACK											X						
FPT_TST.1	X	X								X							
FTP_ITC.1/CoSign-Client								X									
FTP_ITC.1/PRI-APPL-INC-SIGKEY		X	X						X	X						X	
FTP_ITC.1/ALT-APPL-INC-SIGKEY		X	X						X	X						X	
FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY		X	X						X	X						X	
FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY		X	X						X	X						X	
FTP_ITC.1/Radius-Server											X						
FTP_TRP.1											X	X	X	X			

Table 11 - Security Requirement to TOE Security Objective Mapping

6.3.2 Security Requirements tracing justification

The following section provides justification for the above mapping.

OT.Lifecycle_Security (Lifecycle security). The test functions *FPT_TST.1* provide failure detection throughout the lifecycle.
SCD/SVD generation *FCS_CKM.1/SIGNATURE-KEY*, SCD usage *FCS_COP.1/SIGNING*, SCD destruction *FCS_CKM.4* and *FMT_REV.1/SCD* ensure cryptographically secure lifecycle of the SCD.
FDP_ACC.1/Pesonalization SFP, FDP_ACF.1/Pesonalization SFP, FDP_ACC.1/Activation SFP, FDP_ACC.1/SEAL-Activation SFP, FDP_ACF.1/Activation SFP, FDP_ACF.1/SEAL-Activation SFP, FDP_ACC.1/SCD-GEN SFP, FDP_ACF.1/SCD-GEN SFP, FDP_ACC.1/SEAL-SCD-GEN SFP, FDP_ACF.1/SEAL-SCD-GEN SFP,FDP_ACC.1/SVD-Transfer SFP, FDP_ACF.1/SVD-Transfer SFP, FDP_ACC.1/Cert-IMP SFP, FDP_ACF.1/Cert-IMP SFP provides Lifecycle security for the SCD as well as the User account.
The SCD usage is ensured by access control *FDP_ACC.1/Signature-creation SFP*, *FDP_ACF.1/Signature-creation SFP, FDP_ACC.1/SEAL-creation SFP*, *FDP_ACF.1/SEAL-creation SFP* which is based on the security attribute secure TSF management according to *FMT_MOF.1*, *FMT_MSA.1/Users-Administrator*, *FMT_MSA.1/Signatory, FMT_MSA.1/SEAL-Signatory,FMT_MSA.1/Signatory-SCD-GEN, FMT_MSA.1/SEAL-Signatory-SCD-GEN, FDP_ACC.1/Revoke-SCD SFP, FDP_ACF.1/Revoke-SCD SFP, FDP_ACC.1/SEAL-Revoke-SCD SFP, FDP_ACF.1/SEAL-Revoke-SCD SFP, FMT_MSA.1/Signatory-SCD-DISABLE, FMT_MSA.1/Signatory-SCD-NO-REVERT, FMT_MSA.1/SEAL-Signatory-SCD-DISABLE, FMT_MSA.1/SEAL-Signatory-SCD-NO-REVERT , FMT_MSA.1/Signatory-CERT-IMP*, FMT_MSA.2*/Activation-Password-Data*, *FMT_MSA.2/SCD-STATUS*, *FMT_MSA.2/Static-Password-RAD*, *FMT_MSA.2/Static-Password-Data*, *FMT_MSA.3*, *FMT_SMF.1* and *FMT_SMR.1*.
FDP_ACC.1/Revoke-User SFP, FDP_ACF.1/Revoke-User SFP, and *FMT_REV.1/User* provide revocation to the user account as well as all the user's SCDs.
FDP_ACC.1/Unlock-User SFP, *FDP_ACF.1/Unlock-User SFP, FDP_ACC.1/Enable-User SFP*, *FDP_ACF.1/Enable-User SFP, FDP_ACC.1/Disable-User SFP*, *FDP_ACF.1/Disable-User SFP,* will disable the user from performing any operation until an administrator choose to let the user continue without enrolling for a new signature key.
FAU_GEN.1, FAU_GEN.2 and *FPT_STM.1* report any security related issue.

OT.SCD_Secrecy (Secrecy of signature-creation data). OT.SCD_Secrecy is provided by the security functions specified by *FDP_ACC.1/SCD-GEN SFP* and

FDP_ACF.1/SCD-GEN SFP, FDP_ACC.1/SEAL-SCD-GEN SFP and *FDP_ACF.1/SEAL-SCD-GEN SFP* that ensure that only authorised user can generate an SCD. *FCS_CKM.1/SYMMETRIC-KEY, FCS_COP.1/AUK-ENCRYPTION* and *FCS_COP.1/KEY-ENCRYPTION makes* sure that the SCD is kept encrypted inside the internal hard disk using an encryption key that is a combination of the Critical key encryption key and the signatory static password.

The authentication and access management functions specified *by FMT_MOF.1*, *FMT_MSA.1(FMT_MSA.1/Signatory-SCD-GEN, FMT_MSA.1/SEAL-Signatory-SCD-GEN, FDP_ACC.1/Revoke-SCD SFP, FDP_ACF.1/Revoke-SCD SFP, FDP_ACC.1/SEAL-Revoke-SCD SFP, FDP_ACF.1/SEAL-Revoke-SCD SFP,FMT_MSA.1/Signatory-SCD-DISABLE, FMT_MSA.1/Signatory-SCD-NO-REVERT, FMT_MSA.1/SEAL-Signatory-SCD-DISABLE, FMT_MSA.1/SEAL-Signatory-SCD-NO-REVERT)*, *FMT_MSA.2(FMT_MSA.2/SCD-Status), FMT_MSA.3* and FMT_SMR.1 ensure that only the signatory can use the SCD and thus avoid that an attacker may gain information on it. The security functions specified by *FMT_REV.1/SCD and FCS_CKM.4* ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD.
When transmitting of SCD information the following SFRs will ensure secrecy of the SCD: *FDP_ETC.2, FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP , FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/HA-ALT-REPL-INC-SIGKEY, FDP_UCT.1/HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/HA-ALT-REPL-INC-SIGKEY, FPT_TDC.1/HIGH-AVAILABILITY,* FTP_ITC.1/PRI-APPL-INC-SIGKEY, FTP_ITC.1/ALT-APPL-INC-SIGKEY, *FDP_IFF.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/SEAL-HA-ALT-REPL-INC-SIGKEY, FDP_UCT.1/ SEAL-HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/ SEAL-HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/SEAL-HA-ALT-REPL-INC-SIGKEY, FPT_TDC.1/SEAL-HIGH-AVAILABILITY,* FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY, FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY. *FDP_SDI.2* makes sure that security related information is checked against a data integrity property before usage. Only after a proper multi-factor authentication based on *FIA_UAU.5 or one factor authentication based on FIA_UAU.2*, the signatory can decrypt the SCD and perform a digital signature operation. The SCD is encrypted using a special AUK that is also encrypted based on a global master secret key and the static password of the signatory. FMT_MSA.1/Signatory-Change-Password will re-encrypt the AUK and thus have also effect on the secrecy of the

SCD. *FPT_TST.1* tests the working conditions of the TOE. *FPT_PHP.3* require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by *FCS_CKM.1/SIGNATURE-KEY* to generate corresponding SVD/SCD pairs. Cryptographic correspondence is provided by *FCS_COP.1/CORRESP*.
Transmitting of SCD information the following SFRs will ensure secrecy of the SCD*: FDP_ETC.2, FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/* HA-ALT-REPL-INC-SIGKEY*, FDP_UCT.1/HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/HA-ALT-REPL-INC-SIGKEY FPT_TDC.1/HIGH-AVAILABILITY,* FTP_ITC.1/PRI-APPL-INC-SIGKEY, FTP_ITC.1/ALT-APPL-INC-SIGKEY, *FDP_ETC.2, FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFF.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/*SEAL-HA-ALT-REPL-INC-SIGKEY*, FDP_UCT.1/ SEAL-HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/ SEAL-HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/SEAL-HA-ALT-REPL-INC-SIGKEY FPT_TDC.1/SEAL-HIGH-AVAILABILITY,* FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY, FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY*.*
FDP_SDI.2 makes sure that security related information is checked against a data integrity property before usage.

OT.Tamper_ID (Tamper detection) is provided by *FPT_PHP.2* by the means of passive detection of physical attacks.

OT.Tamper_Resistance (Tamper resistance) is provided by *FPT_PHP.3* to resist physical attacks.

OT.SCD/SVD_Gen (SCD/SVD generation) addresses that generation of a SCD/SVD pair requires proper user authentication.
FDP_ACC.1/Personalisation SFP, *FDP_ACC.1/Activation SFP, FDP_ACC.1/SEAL-Activation SFP, FDP_ACF.1/Personalisation SFP* , *FDP_ACF.1/Activation SFP* and *FDP_ACF.1/SEAL-Activation SFP* ensures that only when an account is properly setup and activated, the signatory can generate a new SCD.
The SFR *FDP_ACC.1/SCD-GEN SFP*, *FDP_ACF.1/SCD-GEN SFP,* SFR *FDP_ACC.1/SEAL-SCD-GEN SFP*, *FDP_ACF.1/SEAL-SCD-GEN SFP* provide access control for the SCD/SVD generation.
*FIA_ATD.*1 defines RAD as the corresponding user attribute. The TSF specified

by *FIA_UID.1*, *FIA_UAU.1*, *FIA_UAU.2 and FIA_UAU.5* provide user identification and user authentication prior to enabling access to authorized functions.
The attributes of the authenticated user are provided by *FMT_MSA.2/Activation-Password-Data*, *FMT_MSA.2/Static-Password-RAD*, *FMT_MSA.2/Login-Password-Data*, *FMT_MSA.1/Users-Administrator* and *FMT_MSA.3* for static attribute initialization.
Effort to bypass the access control by a frontal exhaustive attack is blocked by *FIA_AFL.1*.

OT.SCD_Unique (Uniqueness of the signature-creation data) implements the requirement of practically unique SCD as laid down in the Directive [1], Annex III, article 1(a) and in [18] article 1 (b), Annex II, which is provided by the cryptographic algorithms specified by *FCS_CKM.1/SIGNATURE-KEY*.

OT.DTBS_Integrity_TOE (Verification of DTBS/R) covers that integrity of the DTBS/R is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms of *FDP_ITC.1/TOE-DTBS/R*, *FDP_ITC.1/TOE-DTBS/R-SEAL*, *FTP_ITC.1/CoSign-Client*, and by *FDP_UIT.1/TOE-DTBS/R and FDP_UIT.1/TOE-DTBS/R-SEAL*. The access control requirements of *FDP_ACC.1/Signature-Creation SFP* and *FDP_ACF.1/Signature-Creation SFP, FDP_ACC.1/SEAL-Creation SFP* and *FDP_ACF.1/SEAL-Creation SFP* keeps unauthorised parties off from altering the DTBS/R.

OT.Sigy_SigF (Signature generation function for the legitimate signatory only) is provided by *FIA_UAU.5* and *FIA_UID.1* that ensure that no signature generation function can be invoked before the signatory is identified and authenticated.

The security functions specified by *FDP_ACC.1/Personalisation SFP , FDP_ACC.1/Activation SFP, FDP_ACC.1/SEAL-Activation SFP, FDP_ACC.1/SCD-GEN SFP, FDP_ACC.1/SEAL-SCD-GEN SFP, FDP_ACC.1/SVD-Transfer SFP, FDP_ACC.1/Cert-IMP SFP, FDP_ACC.1/Signature-Creation SFP, FDP_ACC.1/Seal-Creation SFP , FDP_ACF.1/Personalisation SFP, FDP_ACF.1/Activation SFP, FDP_ACF.1/SEAL-Activation SFP, FDP_ACF.1/SCD-GEN SFP, FDP_ACF.1/SEAL-SCD-GEN SFP, FDP_ACF.1/SVD-Transfer SFP , FDP_ACF.1/Cert-IMP SFP , FDP_ACF.1/Signature-Creation SFP*, *FDP_ACF.1/Seal-Creation SFP , FMT_SMR.1* ensure that the signature process is restricted to the signatory.

The security functions specified by *FIA_ATD.1, FMT_MOF.1, FMT_MSA.2* and *FMT_MSA.3* ensure that the access to the signature generation functions remain under the sole control of the signatory, as well as *FMT_MSA.1/Signatory,*

FMT_MSA.1/SEAL-Signatory, FMT_MSA.1/Signatory-SCD-GEN, FMT_MSA.1/SEAL-Signatory-SCD-GEN, FDP_ACC.1/Revoke-SCD SFP, FDP_ACF.1/Revoke-SCD SFP, FDP_ACC.1/SEAL-Revoke-SCD SFP, FDP_ACF.1/SEAL-Revoke-SCD SFP, FMT_MSA.1/SEAL-Signatory-SCD-DISABLE, FMT_MSA.1/SEAL-Signatory-SCD-NO-REVERT, FMT_MSA.1/Signatory-SCD-DISABLE, FMT_MSA.1/Signatory-SCD-NO-REVERT, FMT_MSA.1/SEAL-Signatory-SCD-DISABLE, FMT_MSA.1/SEAL-Signatory-SCD-NO-REVERT, FMT_MSA.1/Signatory-CERT-IMP provides that the control of corresponding security attributes is under signatory's control.

When transmitting of SCD information the following SFRs will ensure secrecy of the SCD*: FDP_ETC.2, FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/* HA-ALT-REPL-INC-SIGKEY*, FDP_UCT.1/HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/HA-ALT-REPL-INC-SIGKEY, FPT_TDC.1/HIGH-AVAILABILITY*, FTP_ITC.1/PRI-APPL-INC-SIGKEY, FTP_ITC.1/ALT-APPL-INC-SIGKEY, *FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFF.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/*SEAL-HA-ALT-REPL-INC-SIGKEY*, FDP_UCT.1/ SEAL-HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/ SEAL-HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/SEAL-HA-ALT-REPL-INC-SIGKEY, FPT_TDC.1/SEAL-HIGH-AVAILABILITY*, FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY, FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY*.*
FDP_SDI.2 makes sure that security related information is checked against a data integrity property before usage.
The security functions specified by *FIA_AFL.1* provide protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication.

OT.Sig_Secure (Cryptographic security of the electronic signature) is provided by the cryptographic algorithms specified by *FCS_COP.1/SIGNING* which ensures the cryptographic robustness of the signature algorithms. The security functions specified by *FPT_TST.1* ensure that the security functions are performing correctly.
When transmitting of SCD information the following SFRs will ensure secrecy of the SCD*: FDP_ETC.2, FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/* HA-ALT-REPL-INC-SIGKEY*, FDP_UCT.1/HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/HA-ALT-REPL-INC-SIGKEY, FPT_TDC.1/HIGH-AVAILABILITY*, FTP_ITC.1/PRI-APPL-INC-SIGKEY, FTP_ITC.1/ALT-APPL-INC-SIGKEY, *FDP_IFC.1/SEAL-HA-PRI-REPL-*

*INC-SIGKEY SFP, FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFF.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/*SEAL-HA-ALT-REPL-INC-SIGKEY*, FDP_UCT.1/ SEAL-HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/ SEAL-HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/SEAL-HA-ALT-REPL-INC-SIGKEY, FPT_TDC.1/SEAL-HIGH-AVAILABILITY,* FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY, FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY*.*
FDP_ACC.1/Signature-Creation SFP, *FDP_ACF.1/Signature-Creation SFP*, *FDP_ACC.1/SEAL-Creation SFP* and *FDP_ACF.1/SEAL-Creation SFP* makes sure that the integrity of the account and the SCD is maintained prior to signature operation.
FDP_SDI.2 makes sure that security related information is checked against a data integrity property before usage.

OT.Signatory_Auth (*Signatory* authentication based on multifactor Auth) is provided by *FIA_UAU.5* and *FIA_UID.1*. It is mandatory to present the both static password and OTP before any digital signature operation.
FDP_ACC.1/Change-Password SFP and FDP*_ACF.1/Change-Password SFP* enable Signatory to change their static password.
A trusted path from the client application is ensured by *FTP_TRP.1*.
The static password will be validated inside the TOE.
The TOE will call the Radius Server using the Radius protocol.
The Radius Server will callback the appliance for the purpose of OTP validation.
The security and integrity of the callback is ensured by *FTP_ITC.1/Radius-Server, FDP_IFC.1/OTP-VAL-CALLBACK SFP, FDP_IFF.1/OTP-VAL-CALLBACK SFP, FDP_ITC.2/OTP-VAL-CALLBACK, FTP_ITC.1/Radius-Server and FPT_TDC.1/OTP-VAL-CALLBACK*.
The OTP validation will always use the original OTP value and not the one sent from the Radius Server as a callback.
Only after a successful OTP validation, the digital signature operation can be performed.

OT.Seal_Auth (Authentication for the purpose of Seal generation based on single factor Auth) provided by *FIA_UAU.1, FIA_UAU.2* and *FIA.UID.1*,
Relevant only if the TOE is installed as a Seal device.
Only after a proper authentication the signatory can continue and perform a digital seal operation.
FDP_ACC.1/Change-Password SFP and *FDP_ACF.1/Change-Password SFP* enables signatories to change their static password.
A trusted path from the client is ensured by *FTP_TRP.1*.

OT.Admin_Auth (*Administrator authentication prior to any operation)* is provided by *FIA_UAU.1* and *FIA.UID.1*, Only after a proper authentication an administrator can continue and perform its management operation.
Appliance administrators are also get authenticated before any appliance related operation and their access rights is measured via *FDP_ACC.1/Appliance-Admin SFP* and *FDP_ACF.1/Appliance-Admin SFP*
FDP_ACC.1/Change-Password SFP and *FDP_ACF.1/Change-Password SFP* enables administrators to change their static password.
A trusted path from the administrative client is ensured by *FTP_TRP.1*.

OT.Account_Separation (Separation between different user accounts) is provided by using access control for all signatory operations as well as administrative operations. The following SFRs are used:
FDP_ACC.1/Personalisation SFP, FDP_ACC.1/Activation SFP, FDP_ACC.1/SEAL-Activation SFP, FDP_ACC.1/SCD-GEN SFP, FDP_ACC.1/SEAL-SCD-GEN SFP, FDP_ACC.1/Cert-IMP SFP, FDP_ACC.1/Signature-Creation SFP, FDP_ACC.1/SEAL-Creation SFP, FDP_ACC.1/SVD-Transfer SFP, FDP_ACC.1/Unlock-User SFP, FDP_ACC.1/Enable-User SFP, FDP_ACC.1/Disable-User SFP, FDP_ACC.1/Export-Certs SFP, FDP_ACC.1/Export-Gr-Imgs SFP, FDP_ACC.1/Import-Gr-Img SFP, FDP_ACC.1/Revoke-User SFP, FDP_ACF.1/Personalisation SFP, FDP_ACF.1/Activation SFP, FDP_ACF.1/SEAL-Activation SFP, FDP_ACF.1/SCD-GEN SFP, FDP_ACF.1/SEAL-SCD-GEN SFP, FDP_ACF.1/Cert-IMP SFP, FDP_ACF.1/Signature-Creation SFP, FDP_ACF.1/SEAL-Creation SFP, FDP_ACF.1/SVD-Transfer SFP, FDP_ACF.1/Unlock-User SFP, FDP_ACF.1/Enable-User SFP, FDP_ACF.1/Disable-User SFP, FDP_ACF.1/Export-Certs SFP, FDP_ACF.1/Export-Gr-Imgs SFP, FDP_ACF.1/Import-Gr-Img SFP, FDP_ACF.1/Revoke-User SFP.
FDP_ITC.1/TOE-DTBS/R, FDP_ITC.1/TOE-DTBS/R-SEAL, FDP_ITC.1/GRIMG, FDP_ITC.1/CERTIFICATE, FDP_UIT.1/SVD-Transfer, *FDP_UIT.1/TOE-DTBS/R* and *FDP_UIT.1/TOE-DTBS/R-SEAL* makes sure that information sent by the signatory is used by the signatory's account.
FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.2 FIA_UID.1 makes sure that all authentication is related to a specific administrator or signatory account.
FMT_MOF.1, FMT_SMF, FMT_SMT and all variants of *FMT_MSA* make sure that all actions will be using the relevant accounts data and identity.
FPT_TRP.1 will make sure that a relevant administrator or signatory access its only own data and operates upon this data.
FCS_CKM.1/SYMMETRIC-KEY and *FCS_COP.1/KEY-ENCRYPTION* will make sure that the signature keys are kept encrypted using both a system critical key and the static password of the signatory.

OT.Account_Activation (Activating a user account only once) is provided by *FDP_ACC.1/Activation SFP*, *FDP_ACC.1/SEAL-Activation SFP and FDP_ACF.1/Activation SFP* by restricting that it is possible to perform activation to an account only once.

OT.UserAccountDataProtection (Protecting user data when replicated) is provided by the following SFRs.
The following SFRs will ensure secrecy of the account*: FDP_ETC.2, FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/* HA-ALT-REPL-INC-SIGKEY*, FDP_UCT.1/HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/HA-ALT-REPL-INC-SIGKEY, FPT_TDC.1/HIGH-AVAILABILITY,* FTP_ITC.1/PRI-APPL-INC-SIGKEY, FTP_ITC.1/ALT-APPL-INC-SIGKEY.*FDP_SDI.2, FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_IFF.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP, FDP_IFF.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP, FDP_ITC.2/*SEAL-HA-ALT-REPL-INC-SIGKEY*, FDP_UCT.1/ SEAL-HA-PRI-REPL-CONF-INC-SIGKEY, FDP_UCT.1/ SEAL-HA-ALT-REPL-CONF-INC-SIGKEY, FDP_UIT.1/SEAL-HA-ALT-REPL-INC-SIGKEY, FPT_TDC.1/SEAL-HIGH-AVAILABILITY,* FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY, FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY makes sure that security related information is checked against a data integrity property before usage. *FCS_CKM.1/SYMMETRIC-KEY* and *FCS_COP.1/DATA-INTEG* are used for performing the data integrity checks.

OT.Keys&SecretData_Gen (Master keys generation and management) is provided by the following SFRs.

FCS_CKM.1/SYMMETRIC-KEY ensure proper generation of the master keys.

FPT_PHP.2 and *FPT_PHP.3* ensures the protection of the master keys upon a tamper attempt.

6.3.3 Rationale for EAL4 augmented

The assurance level for this protection profile is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly 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 Advanced methodical vulnerability analysis

ALC_FLR.1 Basic flaw remediation

ATE_DPT.2 Testing – security enforcing modules

Information related to AVA_VAN.5

The TOE is intended to function in a variety of signature creation systems for qualified and non qualified electronic signatures. The TOE will be installed in a secure environment of an IT department of an organization. Due to policies such as [1], Advanced methodical vulnerability analysis is required.

The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure. The component AVA_VAN.5 has the following dependencies:

ADV_ARC.1	Security architecture description
ADV_FSP.4	Security-enforcing functional specification
ADV_TDS.3	Basic modular design
ADV_IMP.1	Implementation representation of the TSF
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures

All of these dependencies are met or exceeded in the EAL4 assurance package.

Information related to ALC_FLR.1

The TOE is based on a complex software component that included a variety of software modules. Some of the software modules are based on open source. It is very probable that it will be required to change the software of the TOE due to problems founds in the sources of the TOE. The problems may sometimes reveal security flaws. This can happen either because a problem of the direct developer of the TOE or a problem found in the relying open source that is used by the TOE. Therefore, a mechanism that will enable users of the TOE to install a fixed version of the TOE and having this version certified, within a certification maintenance process, is required.

The component ALC_FLR.1 has no dependencies.

Information related to ATE_DPT.2

The former version of the TOE was evaluated according to CC version 3.1 rev 2, which requires ATE_DPT.2.
For this reason and due to the complexity of the module it was decide to require to have the security enforcement modules tested.

The component ATE_DPT.2 has the following dependencies:

ADV_ARC.1	Security architecture description
ADV_TDS.3	Basic modular design
ATE_FUN.1	Functional testing

7 TOE Summary Specification

To fulfill the Security Functional Requirements, the TOE comprises the following Security Functions (TSF):

1. Access Control
2. Identification and Authentication
3. Cryptographic Operation
4. Secure communication and session management
5. Auditing
6. Tamper detection
7. High availability and disaster recovery
8. Self test

Each of the TOE security functions is described in the following sections in detail.

7.1 Access Control (TSF.ACC)

The access control rights being described below depend on the current user role "Appliance Administrator"(R.ApplianceAdmin), "Users Administrator" (R.UserAdmin) or "Signatory" (R.Sigy).
All access rights that defined below are enforced by the TOE.

1. The TOE makes sure that the creation of a user account is only allowed for an authenticated Users Administrators.
2. The TOE makes sure that the account activation can be done only by the Signatory. The TOE makes sure that if the account is already activated, the account cannot be activated again.
   During activation the signatory sets a static password. The static password length should be at least 6 characters.
3. The TOE makes sure that changing the user static password is allowed only for the Signatory (after successful verification with the existing static password). The TOE makes sure that this operation can be done only for an activated account. Changing a static password of an administrator is similar to the process of changing a static password of a signatory.
4. The TOE makes sure that the generation of the SCD/SVD pair is allowed only for Signatory only if the account is activated for an authenticated signatory.
5. The TOE makes sure that the requesting a certificate from an external CA will generate a signed PKCS#10 request, which will be sent to the CGA. The TOE makes sure that this operation is allowed only for an activated account by an authenticated signatory.
6. The TOE makes sure that the certificate is replied back from the CGA and loaded by the authenticated signatory into the TOE. The TOE makes sure that the certificate is bounded to its matching SCD. The operation set the value of the security attribute "SCD operational" of the SCD to "yes".

7. The TOE makes sure that only authenticated signatory can revoke the SCD he/she owns. This operation will set the security attribute “SCD operational” from “yes” to “no” and will destroy the SCD.
8. The TOE makes sure that the modification of the security attribute “SCD operational” from “no” to “yes” is not allowed.
9. The TOE makes sure that only a Users Administrator can revoke the account of the signatory which will revoke the entire list of SCDs of the signatory.
10. The TOE makes sure that as part of the signature ceremony, the authenticated signatory will be able to retrieve the list of certificates that belongs to the account, as well as the list of graphical images that belongs to the account. The signatory will specify the desired certificate and graphical images to use.
11. The TOE makes sure that signature creation is allowed only for Signatory for DTBS/R that (a) if security attribute “SCD operational” has been set to “yes” and (b) the signatory account is activated.
12. If an account gets locked by the TOE after several authentication failures, the TOE makes sure that only Users administrator can unlock the account. Besides unlocking the account, the TOE makes sure that the authenticated Users Administrators does not change any parameter of the account.
13. The TOE makes sure that the authenticated signatory can upload to the account a new graphical image.
14. The TOE makes sure that the authenticated appliance administrator can perform several administrative functions such as retrieving the audit log, setting system parameters. Some of the operations require physical access to the TOE such as setting time, reset tampering and setting networking parameters. These operations will not require the appliance administrator's authentication and will rely on the protection of the secure environment.
15. The TOE makes sure that beside the above operations no other operations are permitted as well as setting any attribute.
16. The TOE makes sure that enable/disable a user is only allowed for an authenticated Users Administrators.
17. The TOE makes sure that if a user is disabled, the user will not be able to login to his/her account.

7.2 Identification and Authentication (TSF.IA)

1. The TOE identifies users by means of a unique user identifier sent by the user during authentication. Each user can have the following roles: “Appliance Administrator“ (R.ApplianceAdmin), “Users Administrator” (R.UserAdmin) or “Signatory” (R.Sigy).
2. The TOE authenticates the identified Signatory by checking the static password and the OTP sent by the user during authentication. The static password is checked against the RAD stored in the TOE for that uniquely

identified user.
OTP is validated when the TOE is deployed as a Signature Creation Device.

3. The OTP is also validated inside the TOE based on accessing the OTP Radius Server using the Radius protocol. The OTP Radius Server will access the TOE as a callback for validating the OTP.
   The Radius Server will provide OTP device profile for the purpose of OTP validation using the OTP callback executed within the scope of the TOE.
   This communication is secured by the TLS protocol as defined in the following TSF.Comm item §7.4 point number 1.
   OTP is validated when the TOE is deployed as a Signature Creation Device.
4. It is possible to define a certain time period of up to 10 minutes, where after the above two factor authentication (based on the static password validation and the OTP validation mechanism) it will be possible to sign several digital signature operations within the same application without entering neither static password nor OTP.
   It will be possible to define a time period, which is less than 10 minutes.
   This is relevant when the TOE is deployed as a Signature Creation Device.
   This functionality is not applicable to CoSign RESTful interface.
5. When the TOE is installed as a Seal Creation Device, it authenticates the identified Signatory by checking the static password. The static password is checked against the RAD stored in the TOE for that uniquely identified user.
6. Administrators are authenticated only using a static password. When TOE hardware version 8.0 is used - Web Console related operations do not require appliance admin authentication and rely on the protection of the secure environment.
   When TOE hardware version 7.0 is used - TOE Console related operations do not require appliance admin authentication and rely on the protection of the secure environment
7. The TOE provides protection of authentication information by locking the account after a predefined number of consecutive failed authentication attempts.
8. Administrator role is assigned to a user after successful authentication if and only if that role is allowed for the user in the TOE's persistent storage.
9. As part of the accessing any sensitive entity such as the user account, an RSA key or a system parameter, the integrity of the entity is checked. This is done using the special Data Integrity server master key that is used for Triple-DES MAC verification operation. Upon failing to check the integrity of the entity, the relevant operation will fail. For example, when the user tries to login and MAC is invalid, the user will not be able to login and thus cannot continue with any operation such as digital signature.

7.3 Cryptographic Operation (TSF.Crypto)

1. The TSF generate 2048 or 4096 bit cryptographic RSA keys. Random numbers for key generation are provided by an internal RNG which is seeded by a true (physical) random source. This function is compliant with the specifications for random numbers and RSA key generation as specified in [6], [9] and [16].
2. Also, the TSF generate triple-DES keys. This function is compliant with specification [14]. The generated keys can be located inside the tamper device or backup USB tokens or encrypted inside the users database.
3. When a sensitive data item is deleted, the TSF zeroize the data. This applies to the following sensitive data items: users private RSA keys, RAD in persistent storage, symmetric keys and to users passwords data in volatile storage.
4. Each signature key is encrypted in the TOE internal database using an account specific key (AUK). The AUK is also kept encrypted in the internal database based on a key that is built by a global master secret key and the static password of the signatory.
5. The TSF performs RSA digital signature-generation according to PKCS1 v1.5 (padding scheme EMSA-PKCS1-v1_5) [5] with 2048 or 4096 bit keys as specified in [6] and [9]. The DTBS/R is sent by the SCA to the TOE. In the case that a DTBS-Representation should be sent, a hash-value of the DTBS is send to the TOE. The hash value is calculated by the SCA.
   The DTBS-representation is based on performing a hash upon the DTBS using one of the following algorithms: SHA-2 family (SHA-256, SHA-384, SHA-512), which are compliant with [6].
6. The SHA-1 of the static password and a user's salt is kept on the Users Database and is used for the static password validation.
7. The following signature suites that are described in [6] are supported:
   - sha256-with-rsa

   With RSA key sizes of 2048 and 4096 bits.

   In Addition, also the following signature suites are supported by CoSign:
   - sha384-with-rsa
   - sha512-with-rsa

   With RSA key sizes of 2048 or 4096 bits.
8. For every RSA key that is generated by the TSF, a following seed is used:
   - RSA 2048 – 100 bit seed
   - RSA 4096 – 100 bit seed

   The RSA key generation algorithm is based on [9] and is compliant with [6]. Since the requirement in [9] is to execute 8 rounds of Miller-Rabin probabilistic primality test, this proves less than 2^{-100} error probability of improper RSA private key components and thus answers the error probability request in [6].

9. A public exponent of $2^{16}+1$ should be used to be compliant with [6].
10. A software based resistance mechanism is implemented into the digital signature operation for balancing the power consumption as well as the signature operation time.
    There are many side channel resistance mechanisms that are introduced in [11], but since the TOE run in a protected environment, enclosed in a metal box and run simultaneously by many users, a basic mechanism is used.
11. Each object that is not a signature key, such as a graphical image or a certificate is encrypted in the TOE internal database using the encryption master key. Upon every access to the object, the object will be decrypted.
12. The Backup file of the appliance is encrypted with a Triple-DES Master Key. The Integrity of the Backup file is based on a calculating a MAC based on a Triple-DES Master Key.

7.4 Secure communication and session management(TSF.Comm)

1. The main communication between the clients and the TSF is always secure and no un-secured communication from external applications is allowed by the TOE. This communication is implemented using the TLS [8] [15] and [17] protocol. This secure communication guarantees the secrecy and data integrity of the messages to and from the TOE as well as the authentication of the TOE to the external application, which is based on the TLS protocol.
   There are two different client communication channels:
   - **TLS communication – regular client**
     The TLS server key and its matching certificate are loaded as part of the TOE manufacturing process. During manufacturing process, the TLS server key is generated outside the boundary of the TOE and uploaded to the TOE. During manufacturing, a matched TLS server certificate is uploaded to the TOE as well. This TLS Server certificate is expired in year 2030.
     In this type of communication, right after the TLS session is established, the user is authenticated based on a User ID and a password. Depending on the user's information in the TOE's DB the user type (e.g. Users Administrator) the user's permissions are determined.
   - **TLS communication – REST**
     The TLS server key and its matching certificate are loaded by the appliance admin. It may that the TLS server key and its matching certificate will be required to be reloaded when the TLS server certificate is expired.
     The reasoning for not generating this TLS server key and certificate during manufacturing is that REST clients will match the communication identity

of the TOE and the Common-Name of the TLS server certificate. Since it is not known during manufacturing the communication identity of the TOE, the key and certificate cannot be uploaded as part of manufacturing procedures.
Every REST request will include the user ID and the user's static password, this way the TOE can use the TOE's database to determine whether the user has permissions to perform the requested operation.

When the TOE is deployed as a Signature Creation Device, the first type of communication is also used by the OTP Radius server to communicate with the TOE for the purpose of OTP validation. In this case, the appliance will accept communication only from Radius Server based on its IP address.

2. In a High Availability configuration there is a primary TOE and alternate TOEs. This configuration is aimed to provide redundancy in the case of a hardware or software failure to the primary TOE.
   The primary TOE updates the other alternate TOE through a TCP/IP communication where the data integrity of the information as well as the secrecy of the critical data is based on application level security.
3. Special mechanisms ensure that no sensitive parameter such as static password or SCD value can be available in a process memory to other user's session than the signatory.

7.5 Auditing

1. The TOE includes a centralized log file that audits all security related events as specified in table 2.
   Every entry in the log file includes date and time.
   The internal motherboard of the system includes an internal clock that is used queried to attach the current time to the relevant event.
2. The date and time can be changed manually by the appliance administrator using the TOE Web Console (when TOE hardware version 8.0 is used) or TOE's Console (when TOE hardware version 7.0 is used).

7.6 Tamper detection & protection (TSF.Tamper)

1. The TOE implements the security function that resists physical tampering.
   The TOE hardware detects the physical tampering (opening of the TOE enclosure), actively erases sensitive data, and terminates main power. This ensures that the assets are not violated.
   During tamper state all functionality of the TOE is stopped and no service is provided (both signatory ones and administrative ones) even if the TOE is hardware restarted.

When the TOE is hardware restarted it will maintain the tamper state such that the previous tamper condition can be reported.

2. Only after the tamper reason is deeply analyzed, the appliance administrator can reset the tamper state by using a special reset tamper operation and providing the backup USB token.
3. The TSF shall ensure that the LAN interface cannot be used to gain access to RAD and SCD.
   This is also relevant for TOE hardware version 8.0 where there exist an additional network interface for the purpose of Web Console.

7.7 Self tests(TSF.Test)

The TSF provides a suite of the following self tests:

1) Start-up tests:
   a) Hardware POST (Power On Self Tests)
   b) Test for a previous tamper event
   c) Test integrity of executable code by verifying its digital signature

2) Tests run while TOE is operational and providing digital signature service:
   a) Encrypt-decrypt integrity test for each RSA key generated
   b) Test the output of the RNG in compliance with [16].
   c) Test integrity of the user account when read from persistent storage. This is done using the special Data Integrity server master key that is used for Triple-DES MAC verification operation.

If any of the start-up tests fail, the TOE will NOT enter operational state. If any of the continuous tests fail, the suspect data will not be used.

7.8 Appliance admin functions (TSF.Admin)

The TSF provides the following administrative functions:

1) **Download audit log**

   The TOE makes sure that the appliance administrator can download the audit log and inspect any security related problem.

2) **Configure system parameters**

   The TOE makes sure that the appliance administrator can configure variant of system parameters. These parameters refine the functionality of the TOE.

The set of networking related parameters such as the IP address of the appliance are not part of the system parameters.
In the case of CoSIgn hardware version 8.0, these networking related parameters are configured from the Web Based Console and do not require appliance admin authentication.
In the case of CoSIgn hardware version 7.0, these networking related parameters are configured from the TOE's Console and do not require appliance admin authentication.

3) **Upload REST Server TLS Key**

The TOE makes sure that the appliance administrator can upload the TLS Server key of the server side interface of the TOE REST interface

4) **Installing a new alternate appliance**

The TOE makes sure that the appliance administrator can install a new alternate appliance. The installation should be done in a secure environment.

5) **Changing the list of alternate appliances of a primary appliance**

The TOE makes sure that the appliance administrator can remove or add an alternate appliance from the list of alternate appliances of the primary appliance.
This operation is made of the following sub operations:

a) Unsubscribe an alternate appliance – an alternate appliance is removed from the list of alternate appliance of the primary appliance
b) Subscribe an installed alternate appliance – an alternate appliance that was already installed once is listed again as an alternate appliance of a primary appliance.
c) Install an alternate appliance – This operation installs a new alternate appliance and thus adds the new appliance to the list of alternate appliances of the primary appliance
d) Re-initialize an alternate appliance – is basically a technical operation that refreshes the communication between the primary appliance and the alternate appliance and makes sure that the databases are aligned.
e) Get the CoSign appliances information – is basically a technical operation that retrieved appliances data including the primary appliance and its alternates. This information will be retrieved also in the case that the request is sent to an alternate appliance.

6) **Turning an alternate appliance to a primary one**

In the case of emergency, if the primary appliance is not operational, the TOE makes sure that the appliance administrator can turn an alternate appliance to be a primary one, and thus provide service to end users.

7) **Upload Software**

The TOE makes sure that the appliance administrator can upload software updates into the TOE.

8) **Appliance backup**

The TOE makes sure that the appliance administrator can backup appliance data to an encrypted file with data integrity measures.

9) **Appliance restoration**

The TOE makes sure that the appliance administrator can restore a primary appliance based on having the appliance administrator provide a valid Backup USB token and a Backup File as input to the restoration operation.

10) **Shutting down the TOE, Hardware Restarting the TOE or Software Restarting the TOE**

The TOE makes sure that the appliance administrator can shut down the TOE, hardware restart the TOE or software restart the TOE.
In the software restart operation only the main software service of the TOE will stop and start, while in a hardware restart, the operating system of the TOE will be fully shutdown and restart afterwards.

7.9 Rationale for TSF

The following table gives the mapping of the TOE Security Functional Requirements as specified in chapter 6.1 and the TSF described above. The numbers in the table specify the component of the TSF which covers the requirement.

SFR \ TSF	ACC	IA	Crypto	Comm	Auditing	Tamper	Test	Admin
FAU_GEN.1					1			
FAU_GEN.2					1			
FCS_CKM.1/SIGNATURE-KEY			1,7,8				2a	
FCS_CKM.1/SYMMETRIC-KEY		9,2	2					
FCS_CKM.4			3					
FCS_COP.1/CORRESP							2a	
FCS_COP.1/SIGNING			5,7					
FCS_COP.1/DATA-INTEG		9					2c	
FCS_COP.1/AUK-ENCRYPTION			4					
FCS_COP.1/KEY-ENCRYPTION	1	2	4,6					
FCS_COP.1/BKP-DATA-INTEG			12					
FCS_COP.1/BKP-ENCRYPTION			12					
FDP_ACC.1/Personalisation SFP	1							
FDP_ACC.1/Activation SFP	2							
FDP_ACC.1/SEAL-Activation SFP	2							
FDP_ACC.1/SCD-GEN SFP	*4*							
FDP_ACC.1/SEAL-SCD-GEN SFP	*4*							
FDP_ACC.1/Cert-IMP SFP	6							
FDP_ACC.1/Signature-Creation SFP	11							
FDP_ACC.1/SEAL-Creation SFP	11							
FDP_ACC.1/SVD-Transfer SFP	5							
FDP_ACC.1/Unlock-User SFP	12							

SFR \ TSF	ACC	IA	Crypto	Comm	Auditing	Tamper	Test	Admin
FDP_ACC.1/Enable-User SFP	16,17							
FDP_ACC.1/Disable-User SFP	16,17							
FDP_ACC.1/Export-Certs SFP	10							
FDP_ACC.1/Export-Gr-Imgs SFP	10							
FDP_ACC.1/Import-Gr-Img SFP	13							
FDP_ACC.1/Revoke-User SFP	9							
FDP_ACC.1/Appliance-Admin SFP	14							
FDP_ACC.1/Change-Password SFP	3							
FDP_ACC.1/Revoke-SCD SFP	7							
FDP_ACC.1/SEAL-Revoke-SCD SFP	7							
FDP_ACC.1/BACKUP-FILE SFP			12					
FDP_ACF.1/Personalisation SFP	1							
FDP_ACF.1/Activation SFP	2							
FDP_ACF.1/SEAL-Activation SFP	2							
FDP_ACF.1/SCD-GEN SFP	4							
FDP_ACF.1/SEAL-SCD-GEN SFP	4							
FDP_ACF.1/Cert-IMP SFP	6							
FDP_ACF.1/Signature-Creation SFP	11							
FDP_ACF.1/SEAL-Creation SFP	11							
FDP_ACF.1/SVD-Transfer SFP	5							
FDP_ACF.1/Unlock-User SFP	12							
FDP_ACF.1/Enable-User SFP	16,17							
FDP_ACF.1/Disable-User SFP	16,17							
FDP_ACF.1/Export-Certs SFP	10							
FDP_ACF.1/Export-	10							

SFR \ TSF	ACC	IA	Crypto	Comm	Auditing	Tamper	Test	Admin
Gr-Imgs SFP								
FDP_ACF.1/Import-Gr-Img SFP	13							
FDP_ACF.1/Revoke-User SFP	9							
FDP_ACF.1/Appliance-Admin SFP	14							
FDP_ACF.1/Change-Password SFP	3							
FDP_ACF.1/Revoke-SCD SFP	7							
FDP_ACF.1/SEAL-Revoke-SCD SFP	7							
FDP_ACF.1/BACKUP-File			12					8
FDP_ETC.1/SVD Transfer	5							
FDP_ETC.1/Export-Certs	10							
FDP_ETC.1/Export-Gr-Imgs	10							
FDP_ETC.2/HA-PRI-REPL-INC-SIGKEY		9	11	2				
FDP_ETC.2/SEAL-HA-PRI-REPL-INC-SIGKEY		9	11	2				
FDP_ETC.2/BACKUP-FILE			12					8
FDP_ETC.2/BACKUP-FILE-SEAL			12					8
FDP_IFC.1/HA-PRI-REPL-INC-SIGKEY SFP		9	11	2				
FDP_IFC.1/HA-ALT-REPL-INC-SIGKEY SFP		9	11	2				
FDP_IFC.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP		9	11	2				
FDP_IFC.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP		9	11	2				
FDP_IFC.1/OTP-VAL-CALLBACK		3		1				
FDP_IFF.1/HA-PRI-REPL-INC-SIGKEY SFP		9	11	2				
FDP_IFF.1/HA-ALT-REPL-INC-SIGKEY		9	11	2				

SFR \ TSF	ACC	IA	Crypto	Comm	Auditing	Tamper	Test	Admin
SFP								
FDP_IFF.1/SEAL-HA-PRI-REPL-INC-SIGKEY SFP		9	11	2				
FDP_IFF.1/SEAL-HA-ALT-REPL-INC-SIGKEY SFP		9	11	2				
FDP_IFF.1/OTP-VALIDATION-CALLBACK		3		1				
FDP_ITC.1/TOE-DTBS/R	11							
FDP_ITC.1/TOE-DTBS/R-SEAL	11							
FDP_ITC.1/GRIMG	13							
FDP_ITC.1/CERTIFICATE	6							
FDP_ITC.2/HA-ALT-REPL-INC-SIGKEY		9	11	2				
FDP_ITC.2/SEAL-HA-ALT-REPL-INC-SIGKEY		9	11	2				
FDP_ITC.2/ OTP-VALIDATION-CALLBACL		3		1				
FDP_SDI.2		9						
FDP_UCT.1/HA-PRI-REPL-CONF-INC-SIGKEY		9	11	2				
FDP_UCT.1/HA-ALT-REPL-CONF-INC-SIGKEY		9	11	2				
FDP_UCT.1/SEAL-HA-PRI-REPL-CONF-INC-SIGKEY		9	11	2				
FDP_UCT.1/SEAL-HA-ALT-REPL-CONF-INC-SIGKEY		9	11	2				
FDP_UIT.1/SVD-Transfer				1				
FDP_UIT.1/TOE-DTBS/R				1				
FDP_UIT.1/TOE-DTBS/R-SEAL				1				
FDP_UIT.1/HA-ALT-REPL-INC-SIGKEY		9	11	2				
FDP_UIT.1/SEAL-HA-ALT-REPL-INC-		9	11	2				

SFR \ TSF	ACC	IA	Crypto	Comm	Auditing	Tamper	Test	Admin
SIGKEY								
FIA_AFL.1		1,7						
FIA_ATD.1		1,8						
FIA_UAU.1		1,5		1				
FIA_UAU.2		1,2,5		1				
FIA_UAU.5		1,2,3,4		1				
FIA_UID.1		1,6,5		1				
FMT_MOF.1						2		
FMT_MSA.1/Users-Administrator	1							
FMT_MSA.1/Signatory	2-8,10,11, 13							
FMT_MSA.1/SEAL-Signatory	2-8,10,11, 13							
FMT_MSA.1/Signatory-SCD-GEN	4							
FMT_MSA.1/SEAL-Signatory-SCD-GEN	4							
FMT_MSA.1/Signatory-SCD-DISABLE	7							
FMT_MSA.1/SEAL-Signatory-SCD-DISABLE	7							
FMT_MSA.1.1/Signatory-SCD-NO-REVERT	7							
FMT_MSA.1.1/SEAL-Signatory-SCD-NO-REVERT	7							
FMT_MSA.1/Signatory-CERT-IMP	6							
FMT_MSA.1/Signatory- Change-Password	3							
FMT_MSA.1/Admin-Change- Password	3							
FMT_MSA.2/Activation-Password-Data	1							
FMT_MSA.2/SCD-Status	7							
FMT_MSA.2/Static-Password-RAD	3		6					
FMT_MSA.2/Login-Password-Data			6					
FMT_MSA.3	1							
FMT_REV.1/SCD	7							
FMT_REV.1/User	9							
FMT_SMF.1	1,9, ,16					2		1-10
FMT_SMR.1		1						

SFR \ TSF	ACC	IA	Crypto	Comm	Auditing	Tamper	Test	Admin
FPT_PHP.2						1	1b,1c	
FPT_PHP.3						1		
FPT_STM.1					1			
FPT_TDC.1/HIGH-AVAILABILITY		9	11	2				
FPT_TDC.1/SEAL-HIGH-AVAILABILITY		9	11	2				
FPT_TDC.1/OTP-VAL-CALLBACK		3		1				
FPT_TST.1							1	
FTP_ITC.1/CoSign Client				1				
FTP_ITC.1/PRI-APPL-INC-SIGKEY		9	11	2				
FTP_ITC.1/ALT-APPL-INC-SIGKEY		9	11	2				
FTP_ITC.1/SEAL-PRI-APPL-INC-SIGKEY		9	11	2				
FTP_ITC.1/SEAL-ALT-APPL-INC-SIGKEY		9	11	2				
FTP_ITC.1/Radius-Server		3		1				
FTP_TRP.1				1,3		3		

Table 12 - SFR - TSF relationship

8 References

[1] Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures (also referenced in the document as “The Directive”)

[2] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, September 2012 Version 3.1 Rev.4. CCMB-2012-09-001.

[3] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, September 2012 Version 3.1 Rev. 4. CCMB-2012-09-002

[4] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, September 2012 Version 3.1 Rev. 4. CCMB-2012-09-003

[5] RSA Laboratories, PKCS #1: RSA Encryption Standard, An RSA Laboratories Technical Note Version v2.1, Revised June 14, 2002

[6] Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms. ETSI TS102 176-1 V2.1.1 2011-07.

[7] ETSI, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices (ETSI TS102 176-2) V1.2.1. 2005-07.

[8] RFC 2246 - The TLS Protocol, The Internet Society, January 1999

[9] ANSI, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA). X9.31 -1998.

[10] Unused

[11] Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing, Zhou, Feng, http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf

[12] NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General (Revision 3), July 2012.

[13] RFC 2865 – RADIUS (Remote Authentication Dial In User Sevice), The Internet Society, June 2000.

[14] FIPS Publication 46-3 (1999): Data Encryption Standard (DES), National Bureau of Standards.

[15] RFC 5246 - The Transport Layered Security (TLS) Protocol version 1.2, The Internet Society, August 2008

[16] NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators), January 2012

[17] RFC 4346 - The Transport Layered Security (TLS) Protocol version 1.1, The Internet Society, April 2006

[18] eIDAS – electronic identification and trust services for electronic transactions in the internal market. July 2014

9 Appendix A – Acronyms

AUK Account Unique Key

CGA Certificate Generation Application

CSP Certificate Service Provider

DI Directory Independent

DTBS Data To Be Signed. All electronic data to be signed including a user message and signature attributes

DTBS-representation Data To Be Signed Representation

DTBS/R Data To Be Signed or its unique representation. Data received by a secure signature creation device as input in a single signature-creation operation.

Note: *DTBS/R is either*
- *a hash-value of the data to be signed (DTBS), or*
- *an intermediate hash-value of a first part of the DTBS complemented with a remaining part of the DTBS, or*
- *the DTBS.*

EAL Evaluation Assurance Level

IT Information Technology

KEK Key Encryption Key

MAC Message Authentication Code

OTP One Time Password

PP Protection Profile

REST Representational State Transfer

RNG	Random Number Generator
SCA	Signature Creation application
SCD	Signature Creation Data. Private cryptographic key stored in the (Qualified) Signature Creation Device or (Qualified) Seal Creation Device under exclusive control by the signatory to create a (Qualified) electronic signature or (Qualified) electronic seal
SDO	Signed Data Object
SVD	Signature Verification Data (in the case when [1] is used) or Signature Validation Data or Seal Validation Data (in the case when [18] is used).
SF	Security Function
SFP	Security Function Policy
SSCD	Secure Signature Creation Device
QSCD	Qualified Signature Creation Device (**Qualified** electronic **Signature Creation Device** as defined in [18])
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	Trust Service Provider
QTSP	Qualified Trust Service Provider