Security Target for Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna

Document Version: 1.6

Date: 15.11.2024

Revision history

Version	Date	Authors	Revision Description
1.0	31.01.2024	Nextsense Ltd.	First Final version
1.1	18.04.2024	Nextsense Ltd.	Corrections based on the findings from the evaluators
1.2	04.06.2024	Nextsense Ltd.	TOE Version update and minor corrections
1.3	15.07.2024	Nextsense Ltd.	TOE Version update and minor corrections
1.4	07.08.2024	Nextsense Ltd.	Minor corrections
1.5	13.09.2024	Nextsense Ltd.	Minor corrections
1.6	15.11.2024	Nextsense Ltd	Minor corrections

Table of Contents

1 ST Introduction

1.1 ST Reference

This ST is identified by the following unique reference:

ST Title:	Security Target of Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM
ST Version	V 1.6
ST Date:	15.11.2024
ST Author:	Nextsense Ltd.

1.2 TOE Reference

The TOE is identified by the following unique reference:

TOE Name	Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM
TOE short name	NSSAM
TOE Version	3.4
Evaluation Criteria	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
Protection Profile(s)	[EN 419241-2]
Evaluation Assurance Level	EAL 4 augmented by AVA_VAN.5
Developer	Nextsense Ltd.
Evaluation Sponsor	Nextsense Ltd.
Evaluation Facility	CCLab Ltd.
Certification Body	OCSI (Organismo di Certificazione della Sicurezza Informatica) – Italian IT Security Certification Body

1.3 TOE Overview

The TOE[1] is the Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna software component that implements the Signature Activation Protocol (SAP) to obtain user Signature Activation Data (SAD). The TOE uses the SAD from the signer to activate the corresponding signing key for use in a Cryptographic Module (CM). The TOE uses a Cryptographic Module certified according to

[1] For the purpose of this document the term TOE also refers to the terms “NSSAM” or “NSSAM FM Module”.

the protection profile [EN 419221-5], as mandated by the standard [EN 419241-2]. The TOE and the Cryptographic Module are a QSCD as specified in [eIDAS] regulation.

The TOE shares the same tamper protected device and operates inside Thales Luna K7 Cryptographic Module[2] (Thales Luna K7) as a functional module (FM). The TOE uses all Thales Luna K7's crypto functions to operate.

NSSAM module is designed to operate as a part of the Trustworthy System Supporting Server Signing TW4S architecture according to [EN 419241- 1] and to [EN 419241-2]. It integrates with Server Signing Application (SSA) products to provide remote signing functionality to business applications.

The other components of the TW4S system are out of the scope of this ST, it is assumed that they are designed to work and conform to the European Standard [EN 419241-1].

Reference architecture of TW4S according the [EN 419241-1] and to [EN 419241-2] is given in the picture below.

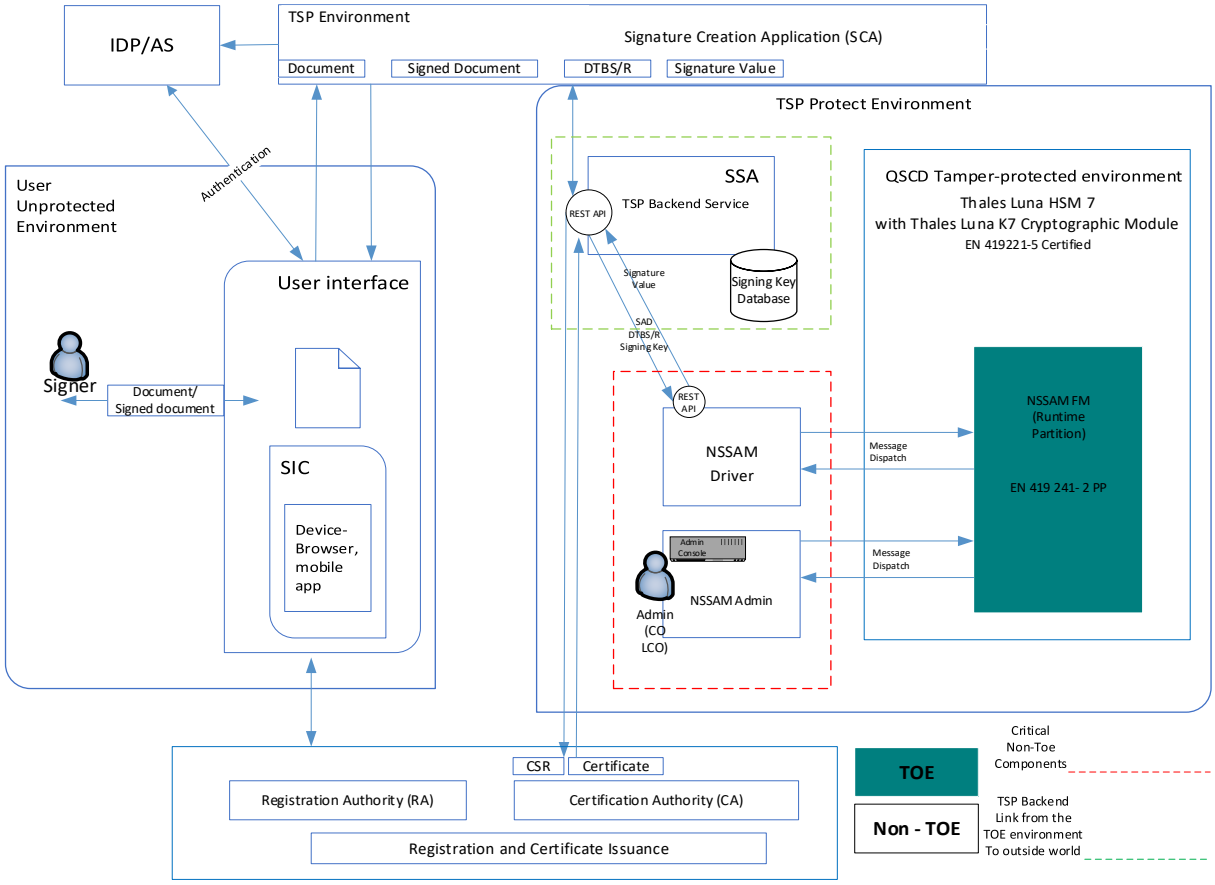


Figure 1: TOE in a TW4S Architecture

The TOE (marked green) is installed within the same HW boundary on the Thales Luna K7.

[2] Thales Luna K7 Cryptographic Module is certified against Protection Profile EN 419221-5:2018, Report Number NSCIB-CC-195307-CR2.

Thales Luna K7 Cryptographic Module is also registered on the EU QSCD list as Thales Luna K7 Cryptographic Module (firmware version: 7.7.0).with reference CC-20-195307-eIDAS; CC-22-195307-eIDAS.

The Security Target for Thales Luna K7 is referenced in the bibliography as [HSM_ST].

NSSAM Driver is the component that is responsible for translating the requests from external entities, Signature Creation Applications (SCA) and forwarding them to the TOE. Every operational request goes through the NSSAM Driver, there is no direct connection between the TOE and external entities. NSSAM Driver basically translates the REST API calls to specific protocols that can be forwarded to the TOE and all business logic (identification, authentication, key generation and signature creation) is done by the TOE.

NSSAM Driver is responsible for the operational requests. NSSAM Admin[3] is a component that is responsible for the configuration and management of the TOE, by calling the appropriate functions of the TOE. It has a Command Line Interface (CLI), the NSSAM Admin Console. Only the Admins can have access to the NSSAM Admin Console to set up and manage the TOE. NSSAM Driver and NSSAM Admin are components outside the TOE and are used to call the appropriate TOE functions where the business logic resides. NSSAM Admin is only a tool so the Admins can use the TOE easier. All commands are performed in the TOE and all configurations are stored in the TOE.

Signing Key Database is a standard database that contains the Signers data and keys. The keys are generated in the HSM every time and then the sensitive data is encrypted with the specific Admin PINs and HSM keys. After the encryption the keys are exported and stored in the external database. Upon every signing operation the signing keys are loaded back to the HSM's memory, decrypted before the operations, and then deleted from the memory and never persisted or exported in plain text.

1.3.1 TOE Usage and major security features

NSSAM is a software component that is loaded into the HSM - Hardware Security Module designed to implement a Signature Activation Module (SAM) according to the European Standard [EN 419241-2].

The main functionalities of the NSSAM component are:

- Ensure the signer has sole control of their signing keys, which is carried out to authorize the signature operation.
- The SAM activates the signing key within a CM, handling a Signature Activation Protocol (SAP) which requires Signature Activation Data (SAD) to be provided at the local environment.
- The SAM component uses the SAD in order to guarantee with a high level of confidence - SCAL 2- that the signing keys are used under sole control of the signer. The SAD binds together the signer authentication with the signing key and the data to be signed DTBS/R.
- NSSAM is software component loaded at tamper protected environment (HSM conformant with [EN 419221-5]), according to the requirements of [EN 419241-2] standard.

To avoid direct communication all external entities, communicate with the TOE via NSSAM Driver for all operations.

The major security features:

1. Authentication of TOE users

[3] Please note that NSSAM Admin component is not equal to Privileged User Admin. NSSAM Admin is a component consists of multiple modules including NSSAM Admin Console that is used by Privileged Users (Admins) to manage the TOE.

The TOE relies on the identification and authentication of an external identity provider of each user before granting access to their signing keys. The TOE makes additional authorization by implementing key authorization mechanism for each user.

2. Signer Key Pair generation and deletion
   The TOE generates keypairs within an HSM certified according to [EN 419221-5] that can be used to create digital signatures/sealing.

3. Signing
   The TOE can perform signing operations within an HSM certified according to [EN 419221-5].

4. Secure Audit
   Every operation performed with the TOE is reliable logged by the TOE. The logs are then forwarded to the HSM certified audit services where multiple options are available to store or export the logs in the SSA or external storages where the logs could be reviewed in case it is needed. The log storage and review are outside the logical scope of the TOE.

5. Secure communication between the TOE and the SCA
   The TOE provides secure channels to protect data integrity and confidentiality in transition.

The TOE handles data assets as specified in chapter 3.1.

1.3.2 TOE Type

The TOE is the Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna (NSSAM 3.4) is a software component, which implements the SAP. TOE software component is loaded into the tamper protected HSM - Hardware Security Module with Thales Luna K7, as a FM module (functional module).

The TOE uses the SAD from the Signer to activate the corresponding signing key for use in CM.

The TOE and CM are together Qualified Signature Creation Device (QSCD).

1.3.3 TOE Life Cycle

The TOE life cycle consists of successive phase for development, production, preparation and operational use.

1. Development: The TOE developer develops the TOE application and its guidance documentation using any appropriate guidance documentation for components working within the TOE physical boundary, including the CM.
2. Delivery: The TOE is securely delivered from the TOE developer to the customer.
3. Installation and configuration: The customer install and configures the TOE with the appropriate configuration and initialization data according to the Installation guide given as part of the delivery package of NSSAM.
4. Operational phase: In operation, the TOE can be used by Privileged users to create Privileged users and signer users. Privileged users can maintain TOE configuration. Privileged users and signer users may generate signature keys for a signer user. Signer users can supply the data to

be signed to the TOE and authorize a signature creation. Privileged users are defined according the HSM Thales Luna K7 roles, and the operation activities are described in the operational guide.

The TOE end-of-life is out of the scope of this document.

Application Note 1

There are two types of Privileged Users. Admins who manage the TOE and Identity Providers who are authorized to create users. Technically the requests can come from any SCA (signature creation application), but the requests are processed only if a registered IDP approved (signed) it.

1.3.4 TOE Environment

NSSAM 3.4 module together with HSM is aimed to support QTSPs requiring using a QSCD for server signing.

The TOE is expected to:

- Operate as parts of server signing system as specified in [EN 419241-1]
- Be used by a TSP applying security policies as required by TSPs providing signature creation services
- Used in conjunction with TSPs issuing certificates

1.3.5 Available non-TOE Hardware/Software/Firmware

The TOE needs, at least, the following hardware/software/firmware to operate:

- TW4S compliant with [EN 419241-1] and [EN 419241- 2] component supporting the NSSAM 3.4.
- SSA component that handles communications between SAM in the QSCD and SCA.
- An Identity Provider providing signed JSON Web tokens (JWT) to state the authentication and authorization of the users.
- Hardware Security Module: HSM with Thales Luna K7 Cryptographic Module compliant with Common Criteria certified against [EN 419221-5]
- A SIC – Signer Interaction Component used locally by the signer to communicate with the remote systems. Typically, it consists of a web browser, a mobile app with an embedded browser or a desktop application with an embedded browser.
- NSSAM Driver and NSSAM Admin.
- Externally database attached to SSA for HSM encrypted signing keys.

The TOE is an FM Module that is specifically made only for HSM devices with Thales Luna K7 Cryptographic Module compliant with Common Criteria certified against [EN 419221-5]. The procurement and delivery of the HSM device is not related with the TOE, but the TOE does not work on any other device type. The TOE can only be activated on such a device (HSM devices with Thales Luna K7 Cryptographic Module compliant with Common Criteria certified against [EN 419221-5]) with a license activation file that is bound to a certified CM model (Thales Luna K7), firmware version (7.7.0) and a serial number. The serial number for the HSM needs to be provided by the owner of the HSM in order to receive a license activation file for the NSSAM. The Thales Luna K7 HSM with firmware version 7.7.0 can be purchased from Thales official points of sale. The license activation file for the NSSAM is provided, at a request from the user of the TOE.

1.4 TOE Description

1.4.1 Physical Scope

The TOE consists of software component and guidance documents. The TOE parts are as follows:

1. NSSAM 3.4 is distributed as a ZIP file with the name: “NSSAM34.zip”. The ZIP File is accompanied by a textual file with a name: ”zipchecksum.txt” that has the SHA-256 checksum, so that the customer can verify that the received ZIP file has not been modified.
   The ZIP file contains the “NSSAM34.fm” which is the FM Module, a textual file with a name “binchecksum.txt” that contains the SHA-256 checksum of the “NSSAM34.fm”, and a public part of a certificate “fmcert.cer” which corresponds to the private part of the certificate owned by Nextsense used to sign the FM Module. The NSSAM can be inserted into the HSM only if the valid public part of the certificate is referenced.
2. The guidance documents of the TOE [Guidance] are as follows:
   - Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM Operations Guide (NSSAM_Guide_AGD_Operations_v1.4.pdf)
   - Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM Installation Guide (NSSAM_Guide_AGD_Installation_v1.4.pdf)
   - Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM Installation Prerequisites (NSSAM_Guide_AGD_InstallPrerequisites_v1.4.pdf)

The NSSAM34.zip file, zipchecksum.txt and guidance documents can be delivered to the customers on the following ways:

- Downloaded from the Nextsense customer support portal.

  Details on accessing the Nextsense customer support portal are provided in an encrypted email.

- Sent by e-mail, in an encrypted format.

1.4.2 Logical Scope

1.4.2.1 Security Audit

The TOE provides reliable audit logs for all important features. Each audit record contains the event type, the date and time of the event, who performed the operation and whether it was successful or not. The audited operations amongst others are:

- start and stop of the system
- managing users
- login of any users
- signing key generation and deletion
- signing key usage
- update of any configuration of the TOE

The TOE Generates the logs and forwards them to the HSM, which means that logs are transferred outside the TOE logical boundaries, but within the HSM physical boundaries. The HSM keeps the logs in the local filesystem and it can be set to further transfer the logs using a remote syslog server. As

the storage of the logs is outside the TOE logical boundaries, the review of the logs is also performed outside of the logical boundaries of the TOE. The audit records of the TOE are forwarded to the HSM, then are further forwarded to the SSA, the audit records generated by the TOE are stored in the SSA in a transitive way.

1.4.2.2 Cryptographic support

The TOE uses Thales Luna K7 Crypto functionality for cryptographic operations such as key generation, data encryption and decryption, securing communication channels and creating digital signatures. The TOE always generates the keys in the certified crypto module (the Thales Luna K7 crypto module). The operations performed with the keys, such as creating electronic signatures, encryption and decryption of data or securing the communication, are always done within the crypto module.

1.4.2.3 User Data Protection

There is no Signer data stored in the TOE only the Signer identifier and the key that belongs to the user. The keys are stored outside the TOE in an external database encrypted with the HSM partition SKS Master key and the 2 SKS Passwords entered during the TOE initialization, as described in section 1.4.2.4. The Signer is authenticated by an external IdP that issues a signed JWT token. The IdP has to be registered in the TOE with the public key that corresponds to the private key used to sign the JWT. The JWT token, as a Signer authentication data, is checked by the TOE (the signature, the IdP name, the validity: not before, issued at, and expires values).

The keys are also protected with the Signer PIN that is never stored in the TOE, and a particular key can be used only if it is authorized for use within the HSM by the key authorization data (combination of email, issuer name and PIN). Nobody can have access to the keys for signing purposes but the owner that is the only one that knows the PIN. Because the PIN is known ONLY by the signer that is the owner of the keypair, by entering the PIN, the TOE ensures that the user signing with the key is the same user that has initiate the keypair creation (when the particular keypair was created). With this, the PIN is becoming the Signer's authentication factor that is known only by the Signer, but also it is part of the key authorization data used to authorize the key usage. The keys are stored in the Signing Key database of the SSA (see Figure 1).

For the purpose of this document the term "key authorization data" refers to the combination of the email, issuer name (which are data from the IdP signed JWT token) and the Signer PIN.

Privileged User data (Admin passwords and IDP public keys) are stored in the TOE secure filesystem.

1.4.2.4 Identification and authentication

The TOE supports Privileged Users and Signers. Privileged Users are administrators of the TOE or Identity Providers that authenticate the Signer.

The different Admins of the TOE are:

- Thales Crypto Officer (CO) is identified by its Crypto Officer PIN. This role is used to install and configure the TOE on the Thales Luna K7
- Thales Limited Crypto Officer (LCO) is identified by Limited Crypto Officer PIN. This role is used to access the Thales Luna K7 functionality including crypto and audit.

CO and LCO are provided by the Thales Luna K7 but as the TOE runs inside Thales Luna K7 it needs the same CO and LCO passwords as Thales Luna K7.

During the initialization of the TOE, five different passwords need to be entered, maintained separately by 5 different password owners. These passwords cannot be changed after the initialization of the TOE:

- 2 SKS Passwords: There should be 2 SKS password owners, each entering a unique password. These two passwords together are used for encryption of the signer's private keys, in combination with the HSM SMK key.
- 3 Session Passwords: there should be three session password owners, each entering a unique password. These passwords are used for the generation of the Master RSA Key and as Authorisation data for the AES session key. This Master RSA key is created in the HSM. The sessions are signed using this Master RSA key.

The password owners are not treated as Privileged Users, as their only function is to maintain the passwords in a secure way. These passwords are only entered during the setup of the TOE or during a recovery from a backup.

The Signer is always authenticated by an external Identity Provider that fulfils the requirements of delegated authentication defined in [EN 419241-1]. The identity provider (IDP) identifies the Signer and then issues a JWT token which must be signed by the IDP, which is then passed to the TOE, so that the TOE can accept and process it. The JWT token, as a part of itself, contains the Signer's e-mail and the identity provider name. The IDP has to be registered in the TOE with its public key (the private is used to sign the JWT). Only JWT tokens signed by registered IDPs are accepted. Still, to get access to the Signer keypair, the Signer also needs to provide their PIN, so the Signer is authenticated based on the content and the signature of the IDP signed JWT token and the PIN, while the key usage is authorized with a key authorization data (a combination of the email, JWT issuer name and the PIN). The PIN is uniquely connected to a Signer, and only the Signer knows the PIN which must be provided in order to use the keypair of that Signer, which means that the knowledge of the PIN verifies that the Signer is the owner of that particular keypair, and is part of the key authorization data to authorize the use of the Signer keypair.

1.4.2.5 Security Management

The management of the TOE is restricted to privileged users (Admins). The Admins set up, configure and manage the TOE via the NSSAM Admin Console.

1.4.2.6 Protection of TSF

The TOE relies on the physical protection of Thales Luna K7 as it runs within the same HW boundary. Thales Luna K7 erases all its keys in case of tamper is detected including the SAM architectural keys used for data encryption meaning nobody can decrypt the data stored outside the TOE.

The TOE uses reliable timestamps for the logs it creates. It protects the data when it's exchanged between the TOE and other IT systems.

1.4.2.7 Trusted Path/Channels

The TOE uses encrypted channels for communicating with the SCAs. Also, the requests are signed by an IDP. The TOE is loaded and operates as a functional module within the logical and physical security of a Luna HSM 7 as part of the HSM firmware where all internal communication resides.

2 Conformance claims

2.1 Common Criteria Conformance claims

This security target is conformant to Common Criteria version 3.1 revision 5.

More precisely, this security target is:

- CC Part 1 [CC1],
- CC Part 2 extended [CC2],
- CC Part 3 conformant [CC3].

The assurance requirement of this security target is EAL4 augmented. Augmentation results from the selection of:

- AVA_VAN.5 Advanced methodical vulnerability analysis

2.2 Protection Profile conformance

This security target claims strict conformance to the following protection profile:

- Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing [EN 419241-2]

3 Security problem definition

3.1 Assets

The TOE has the following assets, which are to be protected in integrity and confidentiality as described below. The TOE must ensure that whenever an asset persists outside the TOE, the TOE has performed the necessary cryptographic operations to enforce confidentiality and detect if an asset has been modified. Access control to TOE assets outside the TOE is to be enforced by the environment.

R.Signing_Key_Id: The signing key is the private key of an asymmetric key pair used to create a digital signature under the signer's sole control. The signing key can only be used by the Cryptographic Module. The TOE uses the asset R.Signing_Key_Id, which identifies a signing key in the Cryptographic Module. The binding of the R.Signing_Key_Id with R.Signer shall be protected in integrity.

R.Authorisation_Data: is data used by the TOE to activate a signing key in the Cryptographic Module. The signing key is identified by R.Signing_Key_Id. It shall be protected in integrity and confidentiality.

R.SVD: signature verification data is the public part, associated with the signing key, to perform digital signature verification. The R.SVD shall be protected in integrity.

The TOE uses a Cryptographic Module for signing key pair generation. As part of the signing key pair generation, the Cryptographic Module provides the TOE with R.Signing_Key_Id and R.SVD. The TOE provides the R.SVD to the SSA for further handling for the key pair to be certified.

R.DTBS/R: set of data which is transmitted to the TOE for digital signature creation on behalf of the signer. The DTBS/R(s) is transmitted to the TOE. The R.DTBS/R shall be protected in integrity. The transmission of the DTBS/R(s) to the TOE shall require the sending party – Signer – to be authenticated.

R.SAD: signature activation data is a set of data involved in the signature activation protocol, which activates the signature creation data to create a digital signature under the signer's sole control. The R.SAD must combine:

- The signer's strong authentication as specified in [EN 419241-1]

- If a particular key is not implied (e.g a default or one-time key) a unique reference to R.Signing_Key_Id.
- A given R.DTBS/R.

The R.SAD shall be protected in integrity and confidentiality.

Application Note 2

R.SAD includes authentication evidence from IDP that the Signer was authenticated. It also contains the Signer PIN that will be verified before the signature is created. The whole message – including the PIN – is encrypted so protected in confidentiality.

Application Note 3

R.Signing_Key_Id is a combination of issuer and Signer Id. The Signer Id is the signer's email.

R.Signature: is the result of the signature operation and is a digital signature value. R.Signature is created on the R.DTBS/R using R.Signing_Key_Id by the Cryptographic Module under the signer's control as part of the SAP. The R.Signature shall be protected in integrity. The R.Signature can be verified outside TOE using R.SVD.

R.Audit: is audit records containing logs of events requiring to be audited. The logs are produced by the TOE and stored externally. The R.Audit shall be protected in integrity.

R.Signer: is a TOE subject containing the set of data that uniquely identifies the signer within the TOE. The R.Signer shall be protected in integrity and confidentiality.

Application Note 4

The R.Signer doesn't contain any confidential data.

R.Reference_Signer_Authentication_Data: is the set of data used by TOE to authenticate the signer. It contains all the data (e.g. OTP device serial number, phone numbers, protocol settings etc.) and keys (e.g. device keys, verification keys etc.) used by the TOE to authenticate the signer. This may include a SVD or certificate to verify an assertion provided as a result of delegated authentication.

The R.Reference_Signer_Authentication_Data shall be protected in integrity and confidentiality.

Application Note 5

The signer authentication data is a JWT token signed by the IDP. As the JWT is signed it is protected in integrity.

R.TSF_DATA: is the set of TOE configuration data used to operate the TOE. It shall be protected in integrity.

R.Privileged_User is a TOE subject containing the set of data that uniquely identifies a Privileged User within the TOE. It shall be protected in integrity.

R.Reference_Privileged_User_Authentication_Data is the set of data used by the TOE to authenticate the Privileged User. It shall be protected in integrity and confidentiality.

Application Note 6

Privileged User Admins use their PINs and Passwords to connect to the TOE. Passwords and PINs entered at NSSAM Admin Console are protected in integrity and confidentiality.

CO and LCO privileged users are provided by the Thales Luna K7.

Privileged User IDP is authenticated against its signature on a JWT token in the request.

R.Random is random secrets, e.g. keys, used by the TOE to operate and communicate with external parties. It shall be protected in integrity and confidentiality.

3.2 Subjects

The following subjects interact with the TOE.

- Signer, which is the natural or legal person who uses the TOE through the SAP where he provides the SAD and can sign DTBS/R(s) using his signing key in the Cryptographic Module.
- Privileged User, which performs the administrative functions of the TOE and is able to provide a DTBS/R(s) to the TOE as part of the signature operation.

Application Note 7

The TOE defines the following roles:

- Signer - authenticated by the IDP and the PIN, and their key is authorised for usage by their key authorization data before using the signing keys.
- Privileged User: IDP - authenticated by its digital signature.
- Privileged User: Admin – authenticated by their passwords and PINs.

3.3 Threats

The following threats are defined for the TOE. An attacker described in each of the threats is a subject that is not authorised for the relevant operation but may present to the system as an unknown user or as one of the other defined subjects.

3.3.1 Enrolment

The threats during enrolment are:

T.ENROLMENT_SIGNER_IMPERSONATION

An attacker impersonates signer during enrolment. As examples, it could be:

- by transferring wrong R.Signer to TOE from RA
- by transferring wrong R.Reference_Signer_Authentication_Data to TOE from RA

The assets R.Signer and R.Reference_Signer_Authentication_Data are threatened.

Such impersonation may allow a potential incorrect signer authentication leading to unauthorised signature operation on behalf of the signer.

T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED

An attacker is able to obtain whole or part of R.Reference_Signer_Authentication_Data during enrolment. This can be during generation, storage or transfer to the TOE or transfer between signer and TOE. As examples it could be:

- by reading the data
- by changing the data, e.g. to a known value

The asset R.Reference_Signer_Authentication_Data is threatened.

Such data disclosure may allow a potential incorrect signer authentication leading to unauthorised signature operation on behalf of signer.

The threats on enrolment are threats on the environment in case external authentication is supported by the TOE.

T.SVD_FORGERY

An attacker modifies the R.SVD during transmission to the RA or CA. This results in loss of R.SVD integrity in the binding of R.SVD to signing key and to R.Signer.

The asset R.SVD is threatened.

If the CA relies on the generation of the key pair controlled by the TOE as specified in [ETSI EN 319 411-1][4] clause 6.3.3 d) then an attacker can forge signatures masquerading as the signer.

Application Note 8

R.SVD is stored in the TSP database. Whenever the TSP wants to create a CSR, it is signed with the Signer key inside the TOE meaning the public key is verified before the signature so it cannot be modified.

3.3.2 Signer Management

T.ADMIN_IMPERSONATION

Attacker impersonates a Privileged User and updates R.Reference_Signer_Authentication_Data, R.Signing_Key_Id or R.SVD.

The assets R.Reference_Signer_Authentication_Data, R.SVD and R.Signing_Key_Id are threatened. Such data modification may allow a potential incorrect signer authentication leading to unauthorised signature operation on behalf of Signer.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE

Attacker discloses or changes (e. g. to a known value) R.Reference_Signer_Authentication_Data during an update and is able to create a signature.

[4] ETSI EN 319 411-1 is referenced from [EN 419 241-2]. The ST author is aware that there is a new version available of the referenced standard but the new version doesn't contain the reference clause (6.3.3 d) so decided to refer to the original version that [EN 419 241-2] refers to.

The assets R.Reference_Signer_Authentication_Data and R.Signing_Key_Id are threatened.

Such data disclosure may allow a potential incorrect signer authentication leading to unauthorised signature operation on behalf of a Signer.

3.3.3 Usage

This section describes threats to signature operation including authentication.

T.AUTHENTICATION_SIGNER_IMPERSONATION

An attacker impersonates a Signer using forged R.Reference_Signer_Authentication_Data and transmits it to the TOE during SAP and uses it to sign the same or modified DTBS/R(s).

The assets R.Reference_Signer_Authentication_Data, R.SAD and R.Signing_Key_Id are threatened.

T.SIGNER_AUTHENTICATION_DATA_MODIFIED

An attacker is able to modify R.Reference_Signer_Authentication_Data inside the TOE or during maintenance.

The asset R.Reference_Signer_Authentification_Data is threatened.

Such data modification may allow a potential incorrect signer authentication leading to unauthorised signature operation on behalf of a Signer.

T.SAP_BYPASS

An attacker bypasses one or more steps in the SAP and can create a signature without the signer having authorised the operation.

The asset R.SAD is threatened.

T.SAP_REPLAY

An attacker replays one or more steps of SAP and is able to create a signature without the signer having authorised the operation.

The asset R.SAD is threatened.

T.SAD_FORGERY

An attacker forges or manipulates R.SAD during transfer in SAP and is able to create a signature without the signer having authorised the operation.

The asset R.SAD is threatened.

T.SIGNATURE_REQUEST_DISCLOSURE

An attacker obtains knowledge of R.DTBS/R or R.SAD during transfer to TOE.

The assets R.DTBS/R and R.SAD are threatened.

If the R.DTBS/R or R.SAD do not require encrypted data then this threat is mitigated.

T.DTBSR_FORGERY

An attacker modifies R.DTBS/R during transfer to TOE and is able to create a signature on this modified R.DTBS/R without the signer having authorised the operation on this R.DTBS/R.

The asset R.DTBS/R is threatened.

T.SIGNATURE_FORGERY

An attacker modifies R.Signature during or after creation or during transfer outside the TOE.

The asset R.Signature is threatened.

3.3.1 System

T.PRIVILEGED_USER_INSERTION

An attacker is able to create R.Privileged_User including

R.Reference_Privileged_User_Authentication_Data and is able to log on to the TOE as a Privileged User.

The assets R.Privileged_User and R.Reference_Privileged_User_Authentication_Data are threatened.

T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION

An attacker modifies R.Reference_Privileged_User_Authentication_Data and is able to log on to the TOE as the Privileged User.

The asset R.Reference_Privileged_User_Authentication_Data is threatened.

T.AUTHORISATION_DATA_UPDATE

Attacker impersonates a Privileged User and updates R.Authorisation_Data and may be able to activate a signing key.

The assets R.Authorisation_Data and R.Signing_Key_Id are threatened.

T. AUTHORISATION_DATA _DISCLOSE

Attacker discloses R.Authorisation_Data during an update and is able to activate a signing key.

The assets R.Authorisation_Data and R.Signing_Key_Id are threatened.

T.CONTEXT_ALTERATION

An attacker modifies system configuration R.TSF_DATA to perform an unauthorised operation. The assets R.Signing_Key_Id, R.SVD, R.SAD, R.Reference_Signer_Authentication_Data and R.TSF_DATA are threatened.

T.AUDIT_ALTERATION

An attacker modifies system audit and is able to hide the trace of TOE modification or usage.

The assets R.SVD, R.SAD, R.Signer, R.Reference_Signer_Authentication_Data, R.DTBS/R, R.Signature, R.AUDIT and R.TSF_DATA are threatened.

T.RANDOM

An attacker is able to guess system secrets R.RANDOM and able to create or modify TOE objects or participate in communication with external systems.

3.4 Relations between Threats and Assets

The following table provides an overview of the relationships between an asset, associated security properties and threats. For details consult the individual threats in the previous sections.

Asset	Security Dimensions	Threats
R.Signing_Key_Id	Integrity	T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Authorisation_Data	Integrity	T.AUTHORISATION_DATA_UPDATE
	Confidentiality	T.AUTHORISATION_DATA_UPDATE T.AUTHORISATION_DATA _DISCLOSE
R.SVD	Integrity	T.SVD_FORGERY T.ADMIN_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
R.DTBS/R	Integrity	T.SIGNATURE_REQUEST_DISCLOSE T.DTBSR_FORGERY
	Origin authentication	T.DTBSR_FORGERY
R.SAD	Integrity	T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION T.SAP_BYPASS T.SAP_REPLAY T.SAD_FORGERY
	Confidentiality	T.AUTHENTICATION_SIGNER_IMPERSONATION T.DTBSR_FORGERY T.CONTEXT_ALTERATION
R.Signature	Integrity	T.SIGNATURE_FORGERY
R.Audit	Integrity	T.AUDIT_ALTERATION
R.Signer	Integrity	T.ENROLMENT_SIGNER_IMPERSONATION
R.Reference_Signer_Authentication_Data	Integrity	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T. SIGNER_AUTEHNTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION

		T.MAINTENANCE_AUTHENTICATION_DISCLOSE T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION T.AUDIT_ALTERATION
	Confidentiality	T.ENROLMENT_SIGNER_IMPERSONATION T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED T.SIGNER_AUTEHNTICATION_DATA_MODIFIED T.ADMIN_IMPERSONATION T.MAINTENANCE_AUTHENTICATION_DISCLOSE
		T.AUTHENTICATION_SIGNER_IMPERSONATION T.CONTEXT_ALTERATION
R.Privileged_User	Integrity	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
R.Reference_Privileged_User_Authentication_Data	Integrity	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
	Confidentiality	T.PRIVILEGED_USER_INSERTION T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION
R.RANDOM	Integrity	T.RANDOM
	Confidentiality	T.RANDOM
R.TSF_DATA	Integrity	T.CONTEXT_ALTERATION T.AUDIT_ALTERATION

Table1: Relationships between an asset, associated security properties and threats

3.5 Organizational security policy

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

OSP.RANDOM

The TOE is required to generate random numbers that meet a specified quality metric. These random numbers shall be suitable for use as keys, authentication/authorisation data, or seed data for another random number generator that is used for these purposes.

OSP.CRYPTO

The TOE shall only use algorithm, algorithm parameters and key lengths endorsed by recognized authorities as appropriate by TSPs. This includes generation of random numbers, signing key pairs and signatures as well as the integrity and confidentiality of TOE assets.

3.6 Assumptions

A.PRIVILEGED_USER

It is assumed that all personnel administering the TOE are trusted, competent and possess the resources and skills required for the tasks and is trained to conduct the activities he is responsible for.

A.SIGNER_ENROLMENT

The signer shall be enrolled, and certificates managed in conformance with the regulations given in [eIDAS]. Guidance for how to implement an enrolment and certificate management system in conformance with [eIDAS] is given in e.g. [EN 319 411-1] or for a qualified certificate in e.g. [EN 319 411-2].

A.SIGNER_AUTHENTICATION_DATA_PROTECTION

It is assumed that the signer will not disclose his authentication factors.

A.SIGNER_DEVICE

It is assumed that the device and SIC used by a Signer to interact with the SSA and the TOE is under the signer's control for the signature operation, i.e. protected against malicious code.

A.CA

It is assumed that the qualified TSP that issues qualified certificates is compliant with the relevant requirements for qualified TSPs as defined in [eIDAS].

A.ACCESS_PROTECTED

It is assumed that the TOE operates in a protected environment that limits physical access to the TOE to authorised Privileged Users. The TOE software and hardware environment (including client applications) is installed and maintained by Privileged Users in a secure state that mitigates against the specific risks applicable to the deployment environment.

It is assumed that any audit generated by the TOE are only handled by authorised personal in a physical secured environment. The personal that carries these activities should act under established practices.

It is assumed that where copies of data protected by the TOE are managed outside of the TOE, client applications and other entities must provide appropriate protection for that data to a level required by the application context and the risks in the deployment environment.

Application Note 9

The signing keys are stored outside the TOE but they are protected. They are stored in the external database and encrypted with AES key generated and kept in the HSM. The protected data that stored outside the TOE, can only be used within the QSCD tamper protected environment when it's loaded back to the HSM where it can be decrypted. The HSM is secure since it is certified according to [EN 419221-5].

A.AUTH_DATA

It is assumed that the SAP is designed in such a way that the activation of the signing key is under sole control of the signer with a high level of confidence. If SAD is received by the TOE, it must be assumed that the SAD was submitted under the full control of the signer by means that are in possession of the signer.

A.TSP_AUDITED

It is assumed that the TSP deploying the SSA and TOE is a qualified TSP according to article 3 (20) of Regulation (EU) No 910/2014 [eIDAS] and audited to be compliant with the requirements for TSPs given by [eIDAS].

A.SEC_REQ

It is assumed that the TSP establishes an operating environment according to the security requirements for SCAL2 defined in [EN 419241-1].

4 Security Objectives

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

These security objectives reflect the stated intent, counter the identified threats, and take into account the assumptions.

4.1 Security Objectives by TOE

The following security objectives describe security functions to be provided by the TOE.

4.1.1 Enrolment

OT.SIGNER_PROTECTION

The TOE shall ensure that data associated to R.Signer are protected in integrity and if needed in confidentiality.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA

The TOE shall be able to securely handle signature authentication data, R.Reference_Signer_ Authentication_Data, as part of R.Signer.

OT.SIGNER_KEY_PAIR_GENERATION

The TOE shall be able to securely use the Cryptographic Module to generate signer signing key pairs and assign R.Signing_Key_Id and R.SVD to R.Signer.

OT.SVD

The TOE shall ensure that the R.SVD linked to R.Signer is not modified before it is certified.

4.1.2 User Management

OT.PRIVILEGED_USER_MANAGEMENT

The TOE shall ensure that any modification to R.Privileged_User and R.Reference_Privileged_User_Authentication_Data are performed under control of a Privileged User.

OT.PRIVILEGED_USER_AUTHENTICATION

The TOE shall ensure that an administrator with a Privileged User is authenticated before any action on the TOE is performed.

OT.PRIVILEGED_USER_PROTECTION

The TOE shall ensure that data associated to R.Privileged_User are protected in integrity and if needed in confidentiality.

OT.SIGNER_MANAGEMENT

The TOE shall ensure that any modification to R.Signer, R.Reference_Signer_Authentication_Data, R.Signing_Key_Id and R.SVD are performed under control of the Signer or Privileged User.

4.1.3 Usage

OT.SAD_VERIFICATION

The TOE shall verify the SAD. That is, it shall check there is a link between the SAD elements and ensure the signer is strongly authenticated.

OT.SAP

The TOE shall implement the server-side endpoint of a Signature Activation Protocol (SAP), which provides the following:

- Signer authentication
- Integrity of the transmitted SAD.
- Confidentiality of at least the elements of the SAD which contains sensitive information.
- Protection against replay, bypass of one or more steps and forgery.

Application Note 10

The signer authentication is assumed to be conducted according to [EN 419241-1] SCAL.2 for qualified signatures. This means signer authentication can be carried out in one of the following ways:

- Directly by the SAM. In this case, the SAM verifies the signer's authentication factor(s).
- Indirectly by the SAM. In the case, an external authentication service as part of the TW4S or a delegated party that verifies the signer's authentication factor(s) and issues an assertion that the signer has been authenticated. The SAM shall verify the assertion.
- A combination of the two direct or indirect schemes.

The TOE uses a combination of the two schemes. First, the Signer is authenticated by an IDP, after that the Signer's PIN is verified before each signature.

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION

The TOE shall ensure signature authentication data is protected against attacks when transmitted to the TOE which would compromise its use for authentication.

OT.DTBSR_INTEGRITY

The TOE shall ensure that the R.DTBS/R is protected in integrity when transmitted to the TOE.

OT.SIGNATURE_INTEGRITY

The TOE shall ensure that a signature can't be modified inside the TOE.

OT.CRYPTO

The TOE shall only use algorithm, algorithm parameters and key lengths endorsed by recognized authorities. This includes the generation of random numbers, signing key pairs and signatures as well as the integrity and confidentiality of TOE assets.

4.1.4 System

OT.RANDOM

Random numbers generated used by the TOE for use as keys, in protocols or seed data for another random number generator that is used for these purposes shall meet a defined quality metric in order to ensure that random numbers are not predictable and have sufficient entropy.

OT.SYSTEM_PROTECTION

The TOE shall ensure that modification of R.TSF_DATA is authorised by a Privileged User and that unauthorised modification can be detected.

OT.AUDIT_PROTECTION

The TOE shall ensure that modifications to R.AUDIT can be detected.

4.2 Security Objectives for the Operational Environment

OE.SVD_AUTHENTICITY

The operational environment shall ensure the SVD integrity during transmit outside the TOE to the CA.

OE.CA_REQUEST_CERTIFICATE

The operational environment shall ensure that the qualified TSP that issues qualified certificates is compliant with the relevant requirements for qualified TSPs as defined in [eIDAS].

The operational environment shall use a process for requesting a certificate, including SVD and signer information, and CA signature in a way, which demonstrates the signer is in control of the signing key associated with the SVD presented for certification. The integrity of the request shall be protected.

OE.CERTIFICATE_VERFICATION

The operational environment shall verify that the certificate for the R.SVD contains the R.SVD.

OE.SIGNER_AUTHENTICATION_DATA

The signer’s management of authentication factors data outside the TOE shall be carried out in a secure manner.

OE.DELEGATED_AUTHENTICATION

If the TOE has support for and is configured to use delegated authentication then the TSP deploying the SSA and TOE shall ensure that all requirements in [EN 419241-1] SRA_SAP.1.1 are met.

In addition, the TSP shall ensure that:

- the delegated party fulfils all the relevant requirements of this standard and the requirements for registration according to the Regulation (EU) No 910/2014 [eIDAS], or
- the authentication process delegated to the external party uses an electronic identification means issued under a notified scheme that is included in the list published by the Commission pursuant to Article 9 of the Regulation (EU) No 910/2014 [eIDAS]

If the signer is only authenticated using a delegated party, the TSP shall ensure that the secret key material used to authenticate the delegated party to the TOE shall reside in a certified cryptographic module consistent with the requirement as defined in [EN 419241-1] SRG_KM.1.1.

The audit of the qualified TSP according to EN 419241-1 shall provide evidence that any delegated party meets requirements from EN 419241-1 SRA_SAP.1.1. and optionally SRG_KM.1.1 in case the signer is only authenticated using a delegated party.

OE.DEVICE

The device, computer/tablet/smart phone containing the SIC and which is used by the signer to interact with the TOE shall be protected against malicious code. It shall participate using SIC as local part of the SAP and may calculate SAD as described in [EN 419241-1]. It may be used to view the document to be signed.

OE.ENV

The TSP deploying the SSA and TOE shall be a qualified TSP according to article 3 (20) of Regulation (EU) No 910/2014 [eIDAS] and audited to be compliant with the requirements for TSP's given by [eIDAS]. The audit of the qualified TSP shall cover the security objectives for the operational environment specified in this clause.

The TOE shall operate in a protected environment that limits physical access to the TOE to authorised privileged users. The TOE software and hardware environment (including client applications) shall be installed and maintained by Administrators in a secure state that mitigates against the specific risks applicable to the deployment environment, including (where applicable):

- Protection against loss or theft of the TOE or any of its externally stored assets
- Inspections to deter and detect tampering (including attempts to access side-channels, or to access connections between physically separate parts of the TOE, or parts of the hardware appliance)
- Protection against the possibility of attacks based on emanations from the TOE (e.g. electromagnetic emanations) according to risks assessed for the operating environment
- Protection against unauthorised software and configuration changes on the TOE and the hardware appliance
- Protection to an equivalent level of all instances of the TOE holding the same assets (e.g. where a key is present as a backup in more than one instance of the TOE).

OE.CRYPTOMODULE_CERTIFIED

If the TOE is implemented as a local application within the same physical boundary as the cryptographic module defined in [EN 419221-5] then the TOE relies on the cryptographic module for providing a tamper-protected environment and for cryptographic functionality and random number generation.

If the TOE is implemented within a separate physical boundary then the TOE relies on the cryptographic module for cryptographic functionality and random number generation. The physical boundary shall physically protect the TOE conformant to FPT_PHP.1 and FPT_PHP.3 in [EN 419221-5].

OE.TW4S_CONFORMANT

The TOE shall be operated by a qualified TSP in an operating environment conformant with [EN 419241-1].

4.3 Security Problem Definition and Security Objectives

The following tables map security objectives with the security problem definition.

TOE Security Objectives and threats

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD
Enrolment					
T.ENROLMENT_SIGNER_IMPERSONATION		X	X		
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED		X	X		
T.SVD_FORGERY				X	X
Signer Management					
T.ADMIN_IMPERSONATION					
T.MAINTENANCE_AUTHENTICATION_DISCLOSE			X		
Usage					
T.AUTHENTICATION_SIGNER_IMPERSONATION					
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			X		
T.SAP_BYPASS					
T.SAP_REPLAY					
T.SAD_FORGERY					
T.DTBSR_FORGERY					
T.SIGNATURE_FORGERY					
System					
T.AUTHORISATION_DATA_UPDATE					
T.AUTHORISATION_DATA_DISCLOSE					
T.CONTEXT_ALTERATION					
T.AUDIT_ALTERATION					
T.RANDOM					

Table2: TOE Security Objectives and threats 1.

	User Management	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AUTHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	System	OT.RANDOM	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION
Enrolment									
T.ENROLMENT_SIGNER_IMPERSONATION					X				
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCL OSED									
T.SVD_FORGERY									
Signer Management									
T.ADMIN_IMPERSONATION			X		X				
T.MAINTENANCE_AUTHENTICATION_DISCLOSE									
Usage									
T.AUTHENTICATION_SIGNER_IMPERSONATION									
T.SIGNER_AUTHENTICATION_DATA_MODIFIED									
T.SAP_BYPASS									
T.SAP_REPLAY									
T.SAD_FORGERY									
T.DTBSR_FORGERY									
T.SIGNATURE_FORGERY									
System									
T.PRIVILEGED_USER_INSERTION		X	X						
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_D ATA_MODIFICATION		X	X	X					
T.AUTHORISATION_DATA_UPDATE								X	
T.AUTHORISATION_DATA_DISCLOSE								X	
T.CONTEXT_ALTERATION								X	
T.AUDIT_ALTERATION									X
T.RANDOM							X		

Table 3: TOE Security Objectives and threats 2.

	Usage	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO
Enrolment							
T.ENROLMENT_SIGNER_IMPERSONATION							
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOS ED							
T.SVD_FORGERY							X
Signer Management							
T.ADMIN_IMPERSONATION							
T.MAINTENANCE_AUTHENTICATION_DISCLOSE							
Usage							
T.AUTHENTICATION_SIGNER_IMPERSONATION		X					
T.SIGNER_AUTHENTICATION_DATA_MODIFIED			X	X			
T.SAP_BYPASS			X				
T.SAP_REPLAY			X				
T.SAD_FORGERY			X	X			
T.SIGNATURE_REQUEST_DISCLOSURE			X				
T.DTBSR_FORGERY					X		
T.SIGNATURE_FORGERY						X	X
System							
T.PRIVILEGED_USER_INSERTION							
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DAT A_MODIFICATION							
T.AUTHORISATION_DATA_UPDATE							
T.AUTHORISATION_DATA_DISCLOSE							
T.CONTEXT_ALTERATION							
T.AUDIT_ALTERATION							

Table 4: TOE Security Objectives and threats 3.

TOE Security Objectives and Organizational Security Policies.

	Enrolment	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION DATA	OT.SIGNER_KEY_PAIR_GENERATION	OT.SVD	OSP.RANDOM	OSP.CRYPTO
OSP.RANDOM						X	
OSP.CRYPTO							X

Table 5: TOE Security Objectives and Organizational Security Policies

Threats and Security Objectives for the environment.

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTIFICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S.CONFORMANT
Enrolment							
T.ENROLMENT_SIGNER_IMPERSONATION							X
T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOS ED			X	X			
T.SVD_FORGERY	X	X					
Signer Management							
T.ADMIN_IMPERSONATION							
T.MAINTENANCE_AUTHENTICATION_DISCLOSE							
Usage							
T.AUTHENTICATION_SIGNER_IMPERSONATION							
T.SIGNER_AUTHENTICATION_DATA_MODIFIED							

T.SAP_BYPASS		X	
T.SAP_REPLAY		X	
T.SAD_FORGERY	X	X	
T.DTBSR_FORGERY		X	
T.SIGNATURE_FORGERY			
System			
T.PRIVILEGED_USER_INSERTION			
T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DAT A_MODIFICATION			
T.AUTHORISATION_DATA_UPDATE			
T.AUTHORISATION_DATA_DISCLOSE			
T.CONTEXT_ALTERATION			
T.AUDIT_ALTERATION			

Table 6. Threats and Security Objectives for the environment

Security Objectives for the environment and Assumptions and Security Objectives for the environment.

	OE.SVD_AUTHENTICITY	OE.CA_REQUEST_CERTIFICATE	OE.SIGNER_AUTHENTIFICATION_DATA	OE.DEVICE	OE.ENV	OE.CRYPTOMODULE_CERTIFIED	OE.TW4S.CONFORMANT
Organizational Security Policies							
OSP.TSP_AUDITED							X
OSP.RANDOM							
OSP.CRYPTO						X	
Assumptions							
A.PRIVILEGED_USER							X
A.SIGNER_ENROLMENT					X		
A.SIGNER_AUTHENTICATION_DATA_PROTECTION			X				
A.SIGNATURE_REQUEST_DISCLOSURE				X			
A.SIGNER_DEVICE				X			
A.CA		X					

A.ACCESS_PROTECTED		X	
A.AUTH_DATA	X		
A.TSP_AUDITED		X	
A.SEC_REQ			X

Table 7: Security Objectives for the environment and Assumptions and Security Objectives for the environment

4.4 Rational for the Security Objectives

This section provides rationale objectives that cover each threat, organizational security policy and assumption

4.4.1 Threats and objectives

T.ENROLMENT_SIGNER_IMPERSONATION is covered by OT.SIGNER_PROTECTION requiring R.Signer to be protected in integrity and for sensitive parts in confidentiality.

It is also covered by OT.SIGNER_MANAGEMENT requiring the signer to be securely created.

It is also covered by OT.REFERENCE_SIGNER_AUTHENTICATION_DATA requiring the TOE to be able to assign signer authentication data to the signer.

It is also covered by OE.TW4S_CONFORMANT as that requires signer enrolment to be handled in accordance with [Assurance] for level at least substantial.

T.ENROLMENT_SIGNER_AUTHENTICATION_DATA_DISCLOSED is covered by OT.REFERENCE_SIGNER_AUTHENTICATION_DATA requiring that authentication data be securely handled.

It is also covered by OT.SIGNER_PROTECTION requiring that the attributes, including signer authentication data, be protected in integrity and if needed in confidentiality.

It is also covered by OE.SIGNER_AUTHENTICATION_DATA requiring the signer to keep his authentication data secret.

It is also covered by OE.DEVICE requiring the device used by the signer not to disclose authentication data.

T.SVD_FORGERY is covered by OT.SIGNER_KEY_PAIR_GENERATION requiring a Cryptographic Module to generate signer key pair.

It is also covered by OT.SVD requiring the SVD to be protected while inside the TOE.

It is also covered by OT.CRYPTO requiring the usage of endorsed algorithms.

It is also covered by OE.SVD_AUTHENTICITY requiring the environment to protect the SVD during transmit from the TOE to the CA.

It is also covered by OE.CA_REQUEST_CERTIFICATE requiring the certification request to be protected in integrity.

T.ADMIN_IMPERSONATION is covered by OT.SIGNER_MANAGEMENT and OT.PRIVILEGED_USER_AUTHENTICATION requiring any changes to the signer representation and attributes are carried out in an authorised manner.

T.MAINTENANCE_AUTHENTICATION_DISCLOSE is covered by OT.REFERENCE_SIGNER_AUTHENTICATION_DATA requiring that authentication data be securely handled.

T.AUTHENTICATION_SIGNER_IMPERSONATION is covered by OT.SAD_VERIFICATION requiring that the TOE checks the SAD received in the SAP.

T.SIGNER_AUTHENTICATION_DATA_MODIFIED is covered by OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION requiring the SAD transported protected in the SAP.

It is also covered by OT.REFERENCE_SIGNER_AUTHENTICATION_DATA requiring that authentication data be securely handled.

It is also covered by OT.SAP requiring the integrity of the SAD is protected during transmit in the SAP.

T.SAP_BYPASS is covered by OT.SAP requiring that all steps, including SAD verification, of the SAP must completed.

It is also covered by OE.DEVICE requiring the SIC to participate the in SAP.

T.SAP_REPLAY is covered by OT.SAP requiring that the signature activation protocol must be able to resist whole or part of it being replayed.

It is also covered by OE.DEVICE requiring the SIC to participate the in SAP.

T.SIGNATURE_REQUEST_DISCLOSURE is covered by the OT.SAP requiring the protocol to be able to transmit data securely.

T.SAD_FORGERY is covered by OT.SAP requiring the TOE to be able to detect if the SAD has been modified during transmit to the TOE.

It is also covered by OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION requiring signature authentication data to be protected during transmit to the TOE.

It is also covered by OE.SIGNER_AUTHENTICATION_DATA requiring the signer to protect his authentication data.

It is also covered by OE.DEVICE requiring the device used by the signer to participate correctly in the SAP, in particular the device shall not disclose authentication data.

T.DTBSR_FORGERY is covered by OT.DTBSR_INTEGRITY requiring the R.DTBS/R to be protected in integrity during transmit to the TOE.

It is also covered by OE.DEVICE requiring the SIC to participate the in SAP.

T.SIGNATURE_FORGERY is covered by OT.SIGNATURE_INTEGRITY requiring that the signature is protected in integrity inside the TOE.

It is also covered by OT.CRYPTO requiring the usage of endorsed algorithms.

T.PRIVILEGED_USER_INSERTION is covered by OT.PRIVILEGED_USER_MANAGEMENT requiring only Privileged User can create new R.Privileged_User and OT.PRIVILEGED_USER_AUTHENTICATION that requires a Privileged User to be authenticated.

T.REFERENCE_PRIVILEGED_USER_AUTHENTICATION_DATA_MODIFICATION is covered by OT.PRIVILEGED_USER_MANAGEMENT requiring only Privileged User can modify R.Privileged_User and OT.PRIVILEGED_USER_AUTHENTICATION that requires a Privileged User to be authenticated.

It is also covered by OT.PRIVILEGED_USER_PROTECTION requiring the Privileged User to be protected in integrity.T.AUTHORISATION_DATA_UPDATE is covered by OT.SYSTEM_PROTECTION requiring any unauthorised modification to TOE configuration to be detectable. T.AUTHORISATION_DATA_DISCLOSE is covered by OT.SYSTEM_PROTECTION requiring any unauthorised modification to TOE configuration to be detectable. T.CONTEXT_ALTERATION is covered by OT.SYSTEM_PROTECTION requiring any unauthorized modification to TOE configuration to be detectable. T.AUDIT_ALTERATION is covered by OT.AUDIT_PROTECTION requiring any audit modification can be detected. T.RANDOM is covered by OT.RANDOM requiring that random numbers are not predictable and have sufficient entropy.

4.4.2 Organizational security policies and objectives

OSP.RANDOM is covered by OT.RANDOM requiring that random numbers are not predictable and have sufficient entropy.

OSP.CRYPTO is covered by OT.CRYPTO requiring the usage of endorsed algorithms and OE.CRYPTOMODULE_CERTIFIED requiring a cryptographic module to provide a tamper-protected environment and for cryptographic functionality and random number generation.

4.4.3 Assumption and objectives

A.PRIVILEGED_USER is covered by OE.TW4S_CONFORMANT which requires that the system where the TOE operates is compliant with [EN 419241-1] where clause SRG_M.1.8 requires that administrators are trained.

A.SIGNER_ENROLMENT is covered by OE.ENV requiring the TSP to be audited.

A.SIGNER_AUTHENTICATION_DATA_PROTECTION is covered by OE.SIGNER_AUTHENTICATION_DATA requiring the signer to protect his authentication data.

A.SIGNER_DEVICE is covered by OE.DEVICE requiring the signer's device to be protected against malicious code.

A.CA is covered by OE.CA_REQUEST_CERTIFICATE requiring that the CA will issue certificates containing the SVD.

A.ACCESS_PROTECTED is covered by OE.ENV requiring the TOE be operated in an environment with physical access controls.

A.AUTH_DATA is covered by OE.DEVICE requiring the device to participate correctly in the SAP.

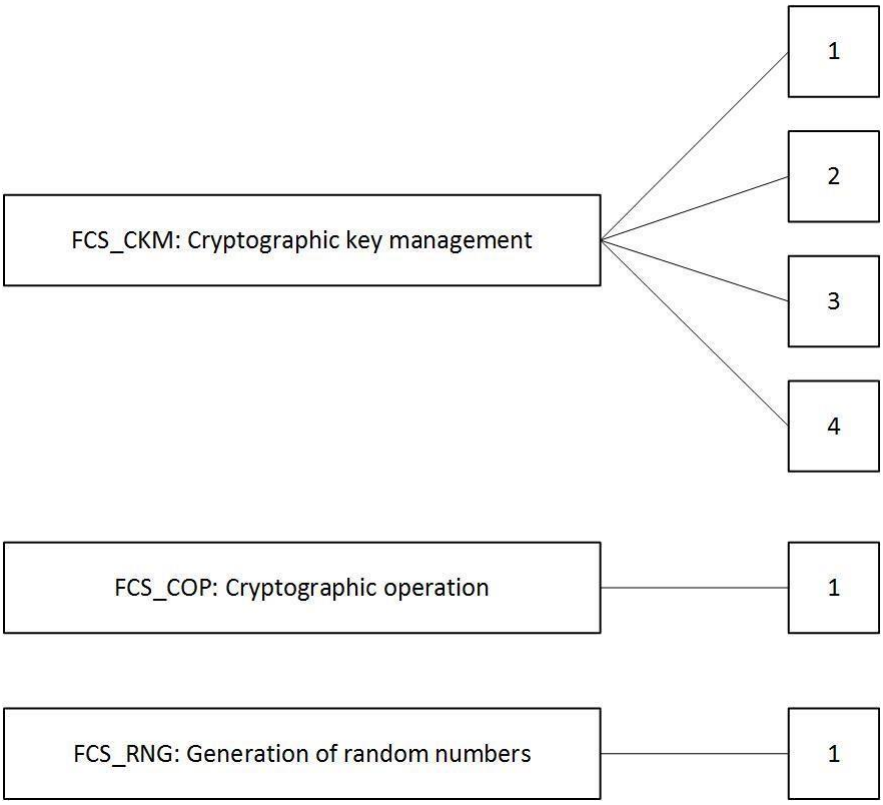
A.TSP_AUDITED is covered by OE.ENV requiring that the TOE is operated by a qualified TSP.

A.SEC_REQ is covered by OE.TW4S_CONFORMANT requiring the system where the TOE operates is compliant with [EN 419241-1].

5 Extended Component Definition

5.1 Class FCS: Cryptographic Support

The Class FCS: Cryptographic Support as defined in [CC2] is extended with a new family: Generation of Random Numbers (FCS_RNG). The family is concerned with the generation of random numbers. The following picture illustrates the decomposition of the Class FCS: Cryptographic Support with the added family FCS_RNG:



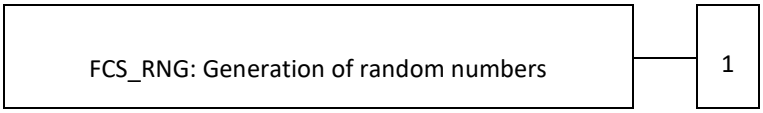
5.1.1 Generation of Random Numbers (FCS_RNG)

This family describes the functional requirements for random number generation used for cryptographic purposes.

Family behaviour:

This family defines quality requirements for the generation of random numbers, which are intended to be use for cryptographic purposes.

Component levelling:



Management:

There are no foreseen management activities.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Generation of random numbers	
Hierarchical to:	No other components.
Dependencies:	No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: list of security capabilities].

FCS_RNG.1.2 The TSF shall provide [selection: bits, octets of bits, numbers [assignment: format of the numbers]] that meet [assignment: a defined quality metric].

6 Security Requirements

6.1 Use of requirement specification

The following conventions are used in the definitions of the SFRs:

Iterations are denoted by a slash "/" and the iteration indicator after the component identifier.

SFR operations from [EN 419241-2] are left as they are in the Protection Profile:

- Refinements are denoted with bold text.
- Selections and assignments are denoted as *italicised*.

ST SFR operations:

- ST operations are the same as the operations in the protection profiles with an additional underline.

6.2 Subjects, Objects and Operations

This section describes the subjects, object and operations supported by the TOE.

Subject	Description
R.Signer	Represents within the TOE the end user that wants to create a digital signature
R.Privileged_User	Represents within the TOE a privileged user that can administer the TOE and a few operations relevant for R.Signer

Table8: Subjects

Object	Description
R.Reference_Privileged_User_Authentication_Data	Data used by the TOE to authenticate a Privileged_User
R.Reference_Signer_Authentication_Data	Data used by the TOE to authenticate a Signer
R.SVD	The public part of a R.Signer signature key pair
R.Signing_Key_Id	An identifier representing the private part of a R.Signer signature key pair
R.DTBS/R	Data to be signed representation
R.Authorisation_Data	Data used by the Cryptographic Module to activate the private part of a R.Signer signature key pair
R.Signature	The result of a signature operation

R.TSF_DATA	TOE Configuration Data

Table9: Objects

Subject	Operation	Object	Description
R.Privileged_User	Create_New_Privilege User	R.Privileged_User R.Reference_Privileged_User_Authentication_Data	A new privileged user can be created which covers the object representing the new privileged user as well as the object used to authenticate the newly created privileged user.
R.Privileged_User	Create_New_Signer	R.Signer R.Reference_Signer_Authentication_Data	A new signer can be created which covers the object representing the new signer as well as the object used to authenticate the newly created signer.
R.Privileged_User R.Signer	Generate_Signer_Key Pair	R.Signer R.SVD R.Signing_Key_Id	A key pair can be generated and assigned to a signer.
R.Privileged User R.Signer	Signer_Maintenance	R.Signer R.SVD R.Signing_Key_Id	A key pair can be deleted from a signer.
~~R.Privileged User~~ **R.Signer**[5]	Supply_DTBS/R	R.Signer R.DTBS/R	Data to be signed by a signer can only be supplied by the signer.
R.Signer	Signing	R.Authorisation_Data R.Signer R.Signing_Key_Id R.DTBS/R R.Signature	A signer can sign data to be signed resulting in a signature.
R.Privileged User	TOE_Maintenance	R.TSF_DATA	The TOE configuration can be maintained by a privileged user.

Table10: Subject, object and operation

6.3 SFR's Overview

Signer object

- FIA_ATD.1 and FIA_USB.1 requires that the R.Signer object is maintained by the TOE.
- FDP_ITC.2/Signer describes the requirements for importing the R.Signer object.
- FDP_ETC.2/Signer describes requirements for exporting the R.Signer object
- FDP_UIT.1 requires the R.Signer object to be protected in integrity when imported and exported.

[5] The TOE doesn't supply DTBS/R. This is allowed according to FDP_ACC.1/Supply DTBS/R SFR.

- FPT_TDC.1 requires the TOE to be able to interpret R.Signer object related data when shared with SSA.
- FMT_MSA.1, FMT_MSA.2 and FMT_MSA.3 describes rules for creation, maintaining and usage of the R.Signer object as well as requirements to its values.

Authentication

- FIA_AFL.1 limit the amount of authentication attempts
- FDP_UCT.1 ensure that access control and information flow data are transmitted in a confidential way.
- FIA_UID.2 and FIA_UAU.1 requires that each user is identified and authenticated before any action on behalf of the user can take place.
- FIA_UAU.5/Signer and FIA_UAU.5/Privileged User describe the list of authentication mechanism.

Create Signer

- FDP_ACC.1/Signer Creation using FDP_ACF.1/Signer Creation describes access control requirements for creating a R.Signer object.
- FIA_USB.1 defines authorization rules for creating new R.Signer objects.

Signer Key Pair Generation

- FDP_ACC.1/Signer Key Pair Generation using FDP_ACF.1/Signer Key Pair Generation describes access control requirements for signing key pair generation.
- FCS_CKM.1/* describe rules for how signing key pair are generated

Signer Key Pair Deletion

- FDP_ACC.1/Signer Key Pair Deletion using FDP_ACF.1/Signer Key Pair Deletion describes access control requirements for signing key pair deletion.
- FCS_CKM.4 requires keys to be securely destructed.

Signer Maintenance

- FDP_ACC.1/Signer Maintenance using FDP_ACF.1/Signer Maintenance describes access control requirements for updating the R.Reference_Signer_Authentication_Data of a R.Signer object.

Supply DTBS/R

- FDP_ACC.1/Supply DTBS/R using FDP_ACF.1/Supply DTBS/R describes access control requirements for a Privileged User to supply a DTBS/R(s).

Signing

- FDP_IFF.1/Signer and FDP_IFC.1/Signer describing requirements on preconditions for a signature operation can be carried out.
- FDP_UIT.1 requires the R.SAD object to be protected from modification and replay.
- FDP_ACC.1/Signing using FDP_ACF.1/Signing describes access control requirements for signing.
- FCS_COP.1/* requires the TOE to perform cryptographic operation conformant with a ST specified list of algorithms.
- FPT_RPL.1 requires detection of replay of the R.SAD and reject signature operation in case of replay detected.
- FPT_STM1 is responsible for reliable time stamps for the signatures.

Privileged User object

- FIA_ATD.1 and FIA_USB.1 requires that the R.Privileged User object is maintained by the TOE.
- FDP_ITC.2/Privileged User describes requirements for importing the R.Privileged User object.
- FDP_ETC.2/ Privileged User describes requirements for exporting the R.Privileged User object
- FDP_UIT.1 requires the R.Privileged User object to be protected in integrity when imported and exported.
- FPT_TDC.1 requires the TOE to be able to interpret R.Privileged User object when shared with a trusted IT product the SSA.
- FMT_MSA.1, FMT_MSA.2, FMT_MSA.3 describes rules for creation, maintaining and usage of the R.Privileged User object as well as requirements to its values.
- FDP_IFC.1/Privileged user and FDP_IFF.1/Privileged User describes rules accessing any of Privileged User's data for Operator.

Privileged User Creation

- FDP_ACC.1/Privileged User Creation using FDP_ACF.1/ Privileged User Creation describes access control requirements for creating a R.Privileged User object.
- FIA_USB.1 defines authorisation rules for creating new R.Privileged User objects.

TOE Maintenance

- FDP_ACC.1/TOE Maintenance using FDP_ACF.1/TOE Maintenance
- FMT_SMF.1, FMT_SMR.2 and FMT_MTD.1 requires the TOE to be able to carry out management functions and maintain users and roles.
- FPT_PHP.1 and FPT_PHP.3 requires the detection of any physical tampering or opening the case that compromises the TOE.

Audit

- FAU_GEN.1 and FAU_GEN.2 describes what shall be audited.

Communication

- FTP_TRP.1/SSA and FTP_TRP.1/SIC requires that either the Privileged User or the Signer initiates the communication.
- FCS_RNG.1 is required to generate random numbers for securing communication channels.
- FTP_ITC.1/CM requires trusted path for communication between SAM and the CM.

6.4 Security Functional Requirements

The individual security functional requirements are specified in the sections below.

6.4.1 Security Audit (FAU)

FAU_GEN.1	Audit Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the *not specified*[6] level of audit; and
c) *Privileged User management;*

[6] [selection: *minimum, basic, detailed, not specified*]

d) *Privileged User authentication;*
e) *Signer management;*
f) *Signer authentication;*
g) *Signing key generation;*
h) *Signing key destruction;*
i) *Signing key activation and usage including the hash of the DTBS/R(s); and R.Signature;*
j) *Change of TOE configuration;*
k) *none*[7].

Application Note 11

TOE records the R.DTBS/R in the audit log.

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, *Type of action performed (success or failure), identity of the role which performs the operation.*[8].

FAU_GEN.2	User identity association
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.

6.4.2 Cryptographic Support (FCS)

FCS_CKM.1/RSA	Cryptographic key generation
FCS_CKM.1.1/RSA	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *RSA*[9] and specified cryptographic key sizes *2048 bits, 4096 bits*[10] that meet the following: *[PKCS#1]*[11].

FCS_CKM.1/ECC	Cryptographic key generation
FCS_CKM.1.1/ECC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECC*[12] and specified

[7] [assignment: *other specifically defined auditable events*]
[8] [assignment: *other audit relevant information*]
[9] [assignment: *cryptographic key generation algorithm*]
[10] [assignment: *cryptographic key sizes*]
[11] [assignment: *list of standards*]
[12] [assignment: *cryptographic key generation algorithm*]

cryptographic curves *NIST P-256, NIST P-384, NIST P-521 bits*[13] that meet the following: [*FIPS 186-4]*[14].

Application Note 12

NSSAM refers to [FIPS 186-4] as in each crypto operation it relies on Thales Luna K7 Cryptographic Modul that also referred to [FIPS 186-4] as that was the latest version of the standard during the certification of Thales Luna K7. [FIPS 186-5] is not changed regarding the algorithms and key sizes that NSSAM uses so it also meets [FIPS 186-5].

FCS_CKM.1/AES	Cryptographic key generation
FCS_CKM.1.1/AES	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES*[15] and specified cryptographic key sizes *256 bits*[16] that meet the following: *Direct generation using FCS_RNG.1*[17].

FCS_CKM.4	Cryptographic key destruction
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *active overwriting of the portion of memory containing the key*[18] that meets the following: *none*[19].

FCS_COP.1/Sign and Verify	Cryptographic operation
FCS_COP.1.1/Sign and Verify	The TSF shall perform *Digital signature generation and verification*[20] in accordance with a specified cryptographic algorithm *RSA; ECDSA*[21] and cryptographic key sizes *For RSA: 2048, 4096; For ECDSA: NIST P-256, NIST P-384, NIST P-521*[22] that meet the following: *For RSA: [PKCS#1]; For ECDSA: [FIPS 186-4]*[23].

FCS_COP.1/Encrypt and Decrypt	Cryptographic operation
FCS_COP.1.1/Encrypt and Decrypt	The TSF shall perform *encryption and decryption*[24] in accordance with a specified cryptographic algorithm *RSA, AES CBC*[25] and cryptographic key sizes *For RSA: 2048 bits, 4096 bits; for AES:* 256 *bits*[26] that meet the following: *For RSA: [PKCS#1]; for AES: [FIPS 197]*[27].

[13] [assignment: *cryptographic key sizes*]
[14] [assignment: *list of standards*]
[15] [assignment: *cryptographic key generation algorithm*]
[16] [assignment: *cryptographic key sizes*]
[17] [assignment: *list of standards*]
[18] [assignment: *cryptographic key destruction method]*
[19] [assignment: *list of standards*]
[20] [assignment: *list of cryptographic operations*]
[21] [assignment: *cryptographic algorithm*]
[22] [assignment: *cryptographic key sizes*]
[23] [assignment: *list of standards*]
[24] [assignment: *list of cryptographic operations*]
[25] [assignment: *cryptographic algorithm*]
[26] [assignment: *cryptographic key sizes*]
[27] [assignment: *list of standards*]

FCS_COP.1/Message digest	Cryptographic operation
FCS_COP.1.1/Message digest	The TSF shall perform *message digest*[28] in accordance with a specified cryptographic algorithm *SHA1, SHA256, SHA384, SHA512* and cryptographic key sizes *not applicable*[29] that meet the following: *[FIPS 180-4]*[30].

FCS_RNG.1 Generation of random numbers	
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2	The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers*]] that meet [assignment: *a defined quality metric*].

Application Note 13

The SFR FCS_RNG.1 does not apply, as the TOE is implemented as a local application within the same physical boundary as the cryptographic module. The SFRs defined in [EN 419221-5] already provide requirements on generation of random numbers.

6.4.3 User Data Protection (FDP)

FDP_ACC.1/Privileged User Creation	Subset access control
FDP_ACC.1.1/Privileged User Creation	The TSF shall enforce the *Privileged User Creation SFP*[31] on: *Subjects: Privileged User* *Objects: New security attributes for the Privileged User to be created.* *Operations: Create_New_Privileged_User* *The TOE creates R.Privileged_User and R.Reference_Privileged_User_Authentication_Data with information transmitted by Privileged User*[32].

Application Note 14

During the TOE initialization the Privileged Users (Admins) are created. NSSAM Admin Console asks for all Admin passwords and PINs during the process.

Later Privileged Users (IDP) can be created by Admins only.

FDP_ACF.1/Privileged User Creation	Security attribute-based access control

[28] [assignment: *list of cryptographic operations*]
[29] [assignment: *cryptographic algorithm*]
[30] [assignment: *list of standards*]
[31] [*assignment:* access control SFP]
[32] [*assignment:* list of subjects and objects controlled under the indicated SFP, and for each, the SFPrelevant security attributes, or named groups of SFP-relevant security attributes]

FDP_ACF.1.1/ Privileged User Creation	The TSF shall enforce the *Privileged User Creation SFP*[33] to objects based on the following: *(1) whether the subject is a Privileged User(Admin) authorized to create a new Privileged User(IDP)*[34]*.*
FDP_ACF.1.2/ Privileged User Creation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User(Admin) who has been authorised for the creation of new users can carry out the Create_New_Privileged_User operation*[35]*.*
FDP_ACF.1.3/ Privileged User Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None*[36]*.*
FDP_ACF.1.4/ Privileged User Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rule: *None*[37]*.*

FDP_ACC.1/Signer Creation	Subset access control
FDP_ACC.1.1/Signer Creation	The TSF shall enforce the *Signer Creation SFP*[38] on: *Subjects: Privileged User* *Objects: R.Signer and* *R.Reference_Signer_Authentication_Data Operations:* *Create_New_Signer*[39]*.*

The TOE creates R.Signer and R.Reference_Signer_Authentication_Data with information transmitted by Privileged User(IDP)[40]

FDP_ACF.1/Signer Creation	Security attribute based access control
FDP_ACF.1.1/ Signer Creation	The TSF shall enforce the *Signer Creation SFP*[41] to objects based on the following: *(1) whether the subject is a Privileged User(IDP) authorized to create a new Signer*[42]*.*

[33] [assignment: *access control SFP*]
[34] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFPrelevant security attributes, or named groups of SFP-relevant security attributes*]
[35] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[36] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[37] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[38] [assignment: access control SFP]
[39] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[40] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[41] [assignment: *access control SFP*]
[42] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

FDP_ACF.1.2/ Signer Creation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User(IDP) who has been authorised for creation of new users can carry out the Create_New_Signer operation*[43].
FDP_ACF.1.3/ Signer Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None*[44].
FDP_ACF.1.4/ Signer Creation	The TSF shall explicitly deny access of subjects to objects based on the following additional rule: *None*[45].

FDP_ACC.1/Signer Maintenance	Subset access control
FDP_ACC.1.1/ Signer Maintenance	The TSF shall enforce the *Signer Maintenance SFP*[46] on: *Subjects: Privileged User and Signer* *Objects: The security attributes R.Reference_Signer_Authentication_Data of R.Signer* *Operations: Signer_Maintenance:* *The Privileged User(IDP) or Signer instructs the TOE to update R.Reference_Signer_Authentication_Data of R.Signer*[47]

FDP_ACF.1/Signer Maintenance	Security attribute-based access control
FDP_ACF.1.1/ Signer Maintenance	The TSF shall enforce the *Signer Maintenance SFP*[48] to objects based on the following: *(1) Whether the subject is a Privileged User or Signer authorised to maintain the Signer security attributes*[49].
FDP_ACF.1.2/Signer Maintenance	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[43] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[44] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[45] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[46] [assignment: *access control SFP*]
[47] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[48] [assignment*: access control SFP*]
[49] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP- relevant security attributes, or named groups of SFP-relevant security attributes*]

	(1) Only a Privileged User or Signer who has been authorised to maintain a Signer can carry out the Signer_Maintenance operation[50].
FDP_ACF.1.3/Signer Maintenance	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *(1) The Signer must be the owner of the R.Signer object to be maintained*[51].
FDP_ACF.1.4/Signer Maintenance	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *(1) If the Signer does not own the R.Signer object, it can't be maintained*[52]

Application Note 15

R.Reference_Signer_Authentication_Data is always a JWT token issued by a registered (within the TOE) identity provider and the Signer PIN. The JWT token contains the Signer identification data, which is the issuer+email. Issuer and e-mail cannot be changed. The PIN however, which is known only to the Signer, can be changed, but only by providing the current PIN and a new PIN.

There is one Signer object created and there is one key pair generated to the Signer during key generation. This data is put together in an encrypted blob and stored outside in the TSP database. There is no maintenance of the Signers except:

- Signers can update their PIN under sole control.
- If the Signer key is blocked due to a wrong PIN provided, Admins can delete the Signer Object from the HSM memory.

FDP_ACC.1/Signer Key Pair Generation	Subset access control
FDP_ACC.1.1/Signing Key Pair Generation	The TSF shall enforce the *Signer Key Pair Generation SFP*: *Subjects: Privileged User and Signer.* *Objects: The security attributes R.SVD and R.Signing_Key_Id as part of R.Signer.* *Operations: Generate_Signer_Key_Pair*

The Privileged User(IDP) or Signer instructs the TOE to request the Cryptographic Module to generate a signing key pair R.Signing_Key_Id and R.SVD and assign them to the R.Signer.

Application Note 16

Authorization Data of the Signer is a combination of the Signer email, JWT Issuer name and the Signer PIN. Authentication Data of the Signer is the signed JWT token issued by the IDP and the Signer PIN. The IDP signs each request coming from the Signer. This IDP signature is verified before processing the

[50] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[51] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[52] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

request. The Signers provide their PIN during key generation and combined with the Signer email and the JWT issuer name is used to create the key authorization data, which in the signing process is used to authorize their signing key in the HSM. Signer provides the PIN during signature creation and if the PIN does not match, the key cannot be authorized and used for signing.

Application Note 17

The signing keys are encrypted with multiple infrastructure keys (two SKS passwords and the SKS Master key (SMK)). The encrypted keys are then sent back to the TSP database. Before every signature created with the key it must be imported back to the HSM where it can be decrypted and used for signing. PIN is needed (to form the key authorization data) for authorizing the key in the HSM and without the authorization it cannot be used for signing. After the signature operation, it is removed from the HSM memory and never leaves it in decrypted format.

FDP_ACF.1/Signer Key Pair Generation	Security attribute based access control
FDP_ACF.1.1/ Signer Key Pair Generation	The TSF shall enforce the *Signer Key Pair Generation SFP*[53] to objects based on the following: *(1) whether the subject is a Privileged User(IDP) or Signer authorised to generate a key pair*[54]*.*
FDP_ACF.1.2/Signer Key Pair Generation	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User(IDP) or Signer who has been authorised to generate the key pair can carry out the Generate_Signer_Key_Pair operation*[55]*.*
FDP_ACF.1.3/Signer Key Pair Generation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *(1) The Signer must be the owner of the R.Signer object where the key pair is to be generated*[56]*.*
FDP_ACF.1.4/Signer Key Pair Generation	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *(1) If the Signer does not own the R.Signer object, key pair shall not be generated*[57]*.*

[53] [assignment: *access control SFP*]

[54] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFPrelevant security attributes, or named groups of SFP-relevant security attributes*]

[55] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[56] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

[57] *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FDP_ACC.1/Signer Key Pair Deletion	Subset access control
FDP_ACC.1.1/Signer Key Pair Deletion	The TSF shall enforce the *Signer Key Pair Deletion SFP*[58] on: *Subjects: Privileged User and Signer* *Objects: The security attributes R.Signing_Key_Id and R.SVD of R.Signer* *Operations: Signer_Key_Pair_Deletion*:

The Privileged User*(Admin)* ~~*or Signer*~~ instructs the TOE to delete the R.Signing_Key_Id and R.SVD from R.Signer[59].

Application Note 18

The key deletion from the external database is not managed by the TOE. The encrypted signing keys are loaded to the HSM by the TOE right before every signing operation. The keys are deleted automatically from the HSM right after the signature is created. If the authorization of the key (with the key authorization data that contains the PIN) failed, the key stays in the HSM. If the failed counter reaches 3, the Admin shall delete manually. Deleting from the external database is the responsibility of the TSP service.

FDP_ACF.1/Signer Key Pair Deletion	Security attribute based access control
FDP_ACF.1.1/Signer Key Pair Deletion	The TSF shall enforce the *Signer Key Pair Deletion SFP*[60] to objects based on the following: *(1) Whether the subject is a Privileged User(Admin) authorised to delete the Signer security attributes*[61].
FDP_ACF.1.2/Signer Key Pair Deletion	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User(Admin) who has been authorised to delete a key pair can carry out the Signer_Key_Pair_Deletion operation*[62].
FDP_ACF.1.3/Signer Key Pair Deletion	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:

[58] [assignment: *access control SFP*]
[59] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[60] [assignment: *access control SFP*]
[61] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[62] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

	(1) The Signer must be the owner of the R.Signer object containing the key pair to be deleted[63]*.*
FDP_ACF.1.4/Signer Key Pair Deletion	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *(1) If the Signer does not own the R.Signer object, the key pair can't be deleted*[64]*.*

The DTBS/R(s) can be supplied to the TOE either by the Signer as part of the Signature Activation Protocol, which is covered by the FDP_ACC.1/Signing or by a Privileged User prior to the signature operation. The following SFR handles the case where the Privileged User supplies the DTBS/R(s).

Application Note 19

The keys are loaded into the TOE right before the signature and deleted from the TOE right after the successful signature operation. The keys are kept in the HSM only if a wrong PIN was provided and the key authorization failed. In that case (after three failed attempts) the Privileged User Admin has the right to delete the key from the HSM. The encrypted signing key object will stay in the SSA external database and it's the responsibility of the SSA (or SSA Administrator) to remove the key object from the database based on the TOE error message.

FDP_ACC.1/Supply DTBS/R	Subset access control
FDP_ACC.1.1/Supply DTBS/R	The TSF shall enforce the *Supply DTBS/R SFP*[65] on: *Subjects: Privileged User* *Objects: The security attributes R.DTBS/R of R.Signer.* *Operations: Supply_DTBS/R*: *The Privileged User(IDP) instructs the TOE to link the supplied DTBS/R(s) to the next signature operation for R.Signer*[66]*.*

Application Note 20

The TOE does not provide facilities to supply the DTBS/R(s) but it signs the DTBS/R the SSA provided.

FDP_ACF.1/Supply DTBS/R	Security attribute-based access control
FDP_ACF.1.1/Supply DTBS/R	The TSF shall enforce the *Supply DTBS/R SFP*[67] to objects based on the following:

[63] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[64] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[65] [assignment: *access control SFP*]
[66] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[67] [assignment: *access control SFP*]

	(1) Whether the subject is a Privileged User authorised to supply a DTBS/R(s)[68]*.*
FDP_ACF.1.2/Supply DTBS/R	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *(1) Only a Privileged User who has been authorised to supply a DTBS/R(s) can carry out the Supply_DTBS/R operation*[69]*.*
FDP_ACF.1.3/Supply DTBS/R	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None*[70]*.*
FDP_ACF.1.4/Supply DTBS/R	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *None*[71]*.*

Application Note 21

The TOE does not provide facilities to supply the DTBS/R(s) but it signs the DTBS/R the SSA provided.

FDP_ACC.1/Signing	Subset access control
FDP_ACC.1.1/Signing	The TSF shall enforce the *Signing SFP*[72] on: *Subjects: Signer* *Objects: R.Authorisation_Data, security attributes R.Signing_Key_Id and R.DTBS/R of R.Signer and R.Signature.* Operations: *Signing:* *The Signer instructs the TOE to perform a signature operation containing the following steps:* • *The TOE establishes R.Authorisation_Data for the R.Signing_Key_Id.* • *The TOE uses the R.Authorisation_Data, and R.Signing_Key_Id to activate a signing key in the Cryptographic Module and signs the R.DTBS/R resulting in R.Signature.* • *The TOE deactivates the signing key when the signature operation is completed*[73]*.*

Application Note 22

The Signer sends their authentication data via the SCA. The JWT token is signed by the IDP. The TOE verifies the IDP signature and if it's valid and not expired. The Signer also sends the PIN. All data is encrypted with a session key generated in the Crypto Module. The data is sent to the Crypto Module

[68] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[69] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[70] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[71] *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[72] [assignment: *access control SFP*]
[73] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

along with the encrypted signing key, which is then decrypted by the use of the SMK key and the 2 SKS Admin Passwords, and authorized by key authorization data. If any of the given keys, passwords, or PIN doesn't match, the key cannot be used.

FDP_ACF.1/Signing	Security attribute based access control
FDP_ACF.1.1/Signing	The TSF shall enforce the *Signing SFP*[74] to objects based on the following: *(1) Whether the subject is a Signer authorised to create a signature*[75]*.*
FDP_ACF.1.2/Signing	The TSF shall enforce the following rules to determine if an operation among Signing controlled subjects and controlled objects is allowed: *(1) The R.SAD is verified in integrity.* *(2) The R.SAD is verified that it binds together the Signer authentication, a set of R.DTBS/R and R.Signing_Key_Id.* *(3) The R.DTBS/R used for signature operations is bound to the R.SAD.* *(4) The Signer identified in the SAD is authenticated according to the rules specified in FIA_UAU.5/Signer.* *(5) Only an R.Signing_Key_Id as bound in the SAD, and which is part of the R.Signer security attributes, can be used to create a signature.*[76]
FDP_ACF.1.3/ Signing	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *(1) The Signer must be the owner of the R.Signer object used to generate the signature*[77]*.*
FDP_ACF.1.4/Signing	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *(1) If the Signer does not own the R.Signer object, it can't be used to create a signature*[78]*.*

FDP_ACC.1/TOE Maintenance	Subset access control
FDP_ACC.1.1/TOE Maintenance	The TSF shall enforce the *TOE Maintenance SFP*[79] on: Subjects: Privileged User Objects: R.TSF_DATA. Operations: TOE_Maintenance:

[74] [assignment: *access control SFP*]
[75] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFPrelevant security attributes, or named groups of SFP-relevant security attributes*]
[76] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[77] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[78] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[79] [assignment: *access control SFP*]

The Privileged User(Admin) transmits information to the TOE to manage R.TSF_DATA[80] .

FDP_ACF.1/TOE Maintenance	Security attribute-based access control
FDP_ACF.1.1/TOE Maintenance	The TSF shall enforce the *TOE Maintenance SFP*[81] to objects based on the following: *(1) Whether the subject is a Privileged User(Admin) authorised to maintain the TOE configuration data*[82]*.*
FDP_ACF.1.2/TOE Maintenance	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: (1) *Only a Privileged User(Admin) who has been authorised to maintain the TOE can carry out the TOE_Maintenance operation*[83].
FDP_ACF.1.3/TOE Maintenance	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *None*[84]*.*
FDP_ACF.1.4/TOE Maintenance	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *None*[85]*.*

FDP_ETC.2/Signer	Export of user data with security attributes
FDP_ETC.2.1/Signer	The TSF shall enforce the *Signer Creation SFP, Signer Key Pair Generation SFP, Signer Key Pair Deletion SFP, Signer Maintenance SFP, Supply DTBS/R SFP and Signing SFP*[86] when exporting user data, controlled under the SFP(s), outside of the TSF.
FDP_ETC.2.2/Signer	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3/ Signer	The TSF shall ensure that the security attributes, when exported outside the TSF, are unambiguously associated with the exported user data.
FDP_ETC.2.4/Signer	The TSF shall enforce the following rules when user data is exported from the TSF: *None*[87].

[80] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[81] [assignment: *access control SFP*]
[82] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[83] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[84] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[85] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[86] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[87] [assignment: *additional exportation control rules*]

Application Note 23

There is no Signer data stored in the TOE. Signer's keypair along with the key attributes are put together in a blob and sent back to the TSP database in the key generation response. The blob is encrypted with HSM infrastructure keys before exporting it.

FDP_IFC.1/Signer	Subset information flow control
FDP_IFC.1.1/Signer	The TSF shall enforce the *Signer Flow SFP*[88] on *Privileged User and Signer accessing Signer security attributes for all operations*[89].

FDP_IFF.1/Signer	Simple security attributes
FDP_IFF.1.1/Signer	The TSF shall enforce the *Signer Flow SFP*[90] based on the following types of subject and information security attributes: *Privileged User and Signer accessing the Signer security attributes*[91].
FDP_IFF.1.2/Signer	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *The TOE shall be initialized with FDP_ACC.1/TOE Maintenance.* *To allow a Signer to sign, the Signer shall be created in the TOE by FDP_ACC.1/Signer Creation followed by FDP_ACC.1/Signer key Pair Generation.* *After Signer is created the following operations can be done: FDP_ACC.1/Signer Key Pair Generation, FDP_ACC.1/Signer Key Pair Deletion, FDP_ACC.1/Supply DTBS/R, FDP_ACC.1/Signer Maintenance and FDP_ACC.1/Signing*[92].
FDP_IFF.1.3/Signer	The TSF shall enforce the: *None*[93].
FDP_IFF.1.4/ Signer	The TSF shall explicitly authorise an information flow based on the following rules: *None*[94].
FDP_IFF.1.5/Signer	The TSF shall explicitly deny an information flow based on the following rules: *None*[95].

[88] [assignment: *information flow control SFP*]
[89] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]
[90] [assignment: *information flow control SFP*]
[91] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[92] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[93] [assignment: *additional information flow control SFP rules*]
[94] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[95] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

FDP_ETC.2/Privileged User	Export of user data with security attributes
FDP_ETC.2.1/Privileged User	The TSF shall enforce the *Privileged User Creation SFP*[96] when exporting user data, controlled under the SFP(s), outside of the TSF.
FDP_ETC.2.2/Privileged User	The TSF shall export the user data with the user data's associated security attributes.
FPP_ETC.2.3/Privileged User	The TSF shall ensure that the security attributes, when exported outside the TSF, are unambiguously associated with the exported user data.
FDP_ETC.2.4/Privileged User	The TSF shall enforce the following rules when user data is exported from the TSF: *None*[97].

Application Note 24

There is no Privileged User data that can be exported from the TOE.

FDP_IFC.1/Privileged User	Subset information flow control
FDP_IFC.1.1/Privileged User	The TSF shall enforce the *Privileged User Flow SFP*[98] on *Privileged User accessing Privileged User security attributes for all operations*[99].

FDP_IFF.1/Privileged User	Simple security attributes
FDP_IFF.1.1/Privileged User	The TSF shall enforce the *Privileged User Flow SFP*[100] based on the following types of subject and information security attributes: *Privileged User accessing the Privileged User security attributes*[101].
FDP_IFF.1.2/Privileged User	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *The TOE shall be initialized with FDP_ACC.1/TOE Maintenance*[102].
FDP_IFF.1.3/Privileged User	The TSF shall enforce the: *None*[103].

[96] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[97] [assignment: *additional exportation control rules*]
[98] [assignment: *information flow control SFP*]
[99] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]
[100] [assignment: *information flow control SFP*]
[101] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[102] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[103] [assignment: *additional information flow control SFP rules*]

FDP_IFF.1.4/Privileged User	The TSF shall explicitly authorise an information flow based on the following rules: *None*[104].
FDP_IFF.1.5/Privileged User	The TSF shall explicitly deny an information flow based on the following rules: *None*[105].

FDP_ITC.2/Signer	Import of user data with security attributes
FDP_ITC.2.1/Signer	The TSF shall enforce the *Signer Creation SFP, Signer Key Pair Generation SFP, Signer Key Pair Deletion, Signer Maintenance SFP, Supply DTBS/R SFP and Signing SFP*[106] when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/Signer	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/Signer	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/Signer	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/Signer	The TSF shall enforce the following rules when importing user data controlled Signer under the SFP from outside the TOE: *None*[107].

Application Note 25

The user's signing key is stored in an external database in encrypted format. This is imported before every signing operation. Other than that, there is no data that is imported to the TOE.

FDP_ITC.2/ Privileged UseImport of user data with security attributes	
FDP_ITC.2.1/Privileged User	The TSF shall enforce the *Privileged User Creation SFP*[108] when importing user data, controlled under the SFP, from outside of the TOE.

[104] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[105] [assignment: *rules, based on security attributes, that explicitly deny information flows*]
[106] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[107] [assignment: *additional importation control rules*]
[108] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

FDP_ITC.2.2/Privileged User	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/Privileged User	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/Privileged User	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/Privileged User	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *None*[109].

Application Note 26

There is an export function provided by the HSM that can export/backup the partition the TOE installed on. This partition is encrypted with the master RSA key meaning the backup file is useless without having the master RSA key. There is a separate function to export the master RSA key. Both export and import functions are available only for Admins.

Other than that, there is no Privileged User data that can be imported to the TOE.

FDP_UCT.1	Basic data exchange confidentiality
FDP_UCT.1.1.	The TSF shall enforce the *Signer Flow SFP and Privileged User Flow SFP* [110] to *transmit and receive*[111] user data in a manner protected from unauthorised disclosure.

FDP_UIT.1	Data exchange integrity
FDP_UIT.1.1	The TSF shall enforce the *Signer Flow SFP and Privileged User Flow SFP*[112] to *transmit and receive*[113] user data in a manner protected from *modification and insertion*[114] errors for R.Signer and R.Privileged User and for R.SAD also[115] from *modification and replay*[116] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether *modification, deletion and insertion*[117] for R.Signer and R.Privileged_User and for R.SAD[118] *whether modification and replay*[119] has occurred.

[109] [[assignment: *additional importation control rules*]
[110] [assignment: *access control SFP(s) and/or information flow control SFP(s)]*
[111] [[selection: *transmit, receive*]
[112] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[113] [selection: *transmit, receive*]
[114] [selection: *modification, deletion, insertion, replay*]
[115] The TSF shall enforce the [*assignment: access control SFP(s) and/or information flow control SFP(s)]* to [selection: *transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors
[116] [selection: *modification, deletion, insertion, replay*]
[117] [selection: *modification, deletion, insertion, replay*]
[118] The TSF shall be able to determine on receipt of user data, whether [selection: *modification, deletion, insertion, replay*] has occurred]
[119] [selection: *modification, deletion, insertion, replay*]

6.4.4 Identification and Authentication (FIA)

FIA_AFL.1	Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when *the number specified in the "Authentication Failure Handling table" below* unsuccessful authentication attempts occur related to *Privileged User(Admin) and Signer authentication*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*[120], the TSF shall *suspend the Privileged User(Admin) and when it is a Signer suspend the usage of R.Signing_Key_Id*[121].

Application Note 27

The details of the suspension are described in the Authentication Failure Handling Table below. For this feature the TOE strongly rely on Thales Luna K7.

Role	**Number of consecutive authentication/authorization failures**	**Functionality being suspended**	**Unblocking condition**
CO	A positive integer within the range [1 to 3], configurable by the Thales Luna K7 SO	CO and LCO are locked out	If the module policy of Thales Luna K7 "Partition SO can reset PIN" is enabled, the Partition SO can unlock the CO role by resetting its authentication data. Otherwise, there is no unblocking capability. All user keys contained in the partition are lost and the CO role must be re-initialized.
LCO	Same as CO	LCO is locked out, CO can still operate	The CO can unlock the LCO role by resetting its credentials.
Signer	3	The related key is blocked: all operations on that key or using that key are forbidden	The CO can unblock the key by setting the number of failed authorizations to any integer value in the range [0...2], or by resetting the key authorization data for General Keys.

Authentication Failure Handling Table

Thales Luna K7 SO and Partition SO are roles of the Thales Luna K7. These are not considered TOE roles. They are required for the preparation and configuration of the environment (Thales Luna K7). More details about Thales Luna K7 roles and configuration can be found in the Thales Luna K7 guidance documents.

[120] [selection: *met, surpassed*]
[121] [assignment: *list of actions*]

FIA_ATD.1	User attribute definition
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: *the security attribute as defined in FIA_USB.1*[122].

FIA_UAU.1	Timing of authentication
FIA_UAU.1.1	The TSF shall allow *initialize operation and export Master RSA public key operation* 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 28

Initialize operation is not available in the operation state. It is only available as a first step of the setup of the TOE. Export Master RSA public key is needed so that the public part of the RSA key that identifies the NSSAM instance to the external entities (applications) can be exported and delivered to the external entities.n

FIA_UAU.5/Signer	Multiple authentication mechanisms
FIA_UAU.5.1/Signer	The TSF shall provide *Authentication by IDP's signature verification, PIN validation,* to support Signer authentication[123].
FIA_UAU.5.2/Signer	The TSF shall authenticate any Signer's[124] claimed identity according to: *IDP's signature verification* and *validation of Signer's PIN*[125].

Application Note 29

Each request that is coming from the Signer contains a JWT token that is signed by an Identity Provider that must have authenticated the signer before signing the JWT token. For key generation requests, the Signer provides a PIN that will be used to further authenticate the Signer (as only Signer themselves know it) and as a part of the key authorization data used to authorize the Signer key inside the HSM. When a request comes from the Signer to create a digital signature, the PIN should also be provided. The PIN is not stored anywhere so if the PIN provided doesn't match the one provided during the key generation, the key could not be authorized so there will be no signature created.

The SAD contains the following data:

- JWT token: signed by the IDP and not expired (it includes the Signer email and Issuer name)
- PIN (that is used to form the key authorization data together with the Signer email and Issuer name)
- DTBS/R

[122] [assignment: list of security attributes]

[123] **The TSF shall provide [assignment: *list of multiple authentication mechanisms*] to support user authentication.**

[124] **user**

[125] **[assignment: *rules describing how the multiple authentication mechanisms provide authentication*]**

FIA_UAU.5/Privileged User	Multiple authentication mechanisms

FIA_UAU.5.1/Privileged User The TSF shall provide *IDP's signature verification* to support Privileged User[126](IDP) authentication.

FIA_UAU.5.2/Privileged User The TSF shall authenticate any user's claimed identity according to the IDP's signature verified against its public key registered by Privileged User Admin.

FIA_UID.2	User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1	User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of the user:

(1) R.Reference_Signer_Authentication_Data
(2) R.Signing_Key_Id
(3) R.SVD
(4) R.Signer
(5) none

to Signer:

(6) R.Reference_Priviliged_User_Authentication_Data
(7) none

to Privileged User[127].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users:

(1) Whether the subject is a Privileged User(IDP) authorized to create a new Signer.
(2) Whether the subject is a Privileged User(Admin) authorized to create a new Privileged User(IDP).
(3) none[128]

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users:

(1) Whether the subject is a Privileged User authorized to modify an R.Signer object.
(2) Whether the subject is a Signer authorized to modify his own R.Signer object.
(3) none[129].

[126] user
[127] [assignment: *list of user security attributes*]
[128] [assignment: *rules for the initial association of attributes*]
[129] [assignment: *rules for the changing of attributes*]

6.4.5 Security Management (FMT)

FMT_MSA.1/Signer	Management of security attributes

FMT_MSA.1.1/Signer The TSF shall enforce the:

(1) Signer Creation SFP[130] to restrict the ability to create[131] the security attributes listed in FIA_USB.1 for Signer[132] to authorised Privileged User[133].

(2) Generate Signer Key Pair SFP[134] to restrict the ability to generate[135] the security attributes R.SVD and R.Signing_Key_Id[136] to authorised Privileged User and Signer[137].

(3) Signer Key Pair Deletion SFP[138] to restrict the ability to destruct[139] the security attribute R.SVD and R.Signing_Key_Id as part of R.Signer[140] to authorised Signer or Privileged User(Admin)[141]

(4) Supply DTBS/R SFP[142] to restrict the ability to create[143] the security attribute R.DTBS/R as part of R.Signer[144] to authorised Privileged User[145]

(5) Signing SFP[146] to restrict the ability to create[147] the security attribute R.DTBS/R as part of R.Signer to authorised Signer[148].

(6) Signing SFP[149] to restrict the ability to query[150] the security attributes as listed in FIA_USB.1 to authorised Signer[151].

(7) Signer Maintenance SFP[152] to restrict the ability to change[153] the security attributes R.Reference_Signer_Authentication_Data[154] as part of R.Signer to authorised ~~Privileged User and~~ Signer[155].

---

130 [assignment: *access control SFP(s), information flow control SFP(s)*]]
131 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
132 [[assignment: *list of security attributes*]
133 [assignment: *the authorised identified roles*]
134 [assignment: *access control SFP(s), information flow control SFP(s)*]
135 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
136 [assignment: *list of security attributes*]
137 [assignment: *the authorised identified roles*]
138 [assignment: *access control SFP(s), information flow control SFP(s)*]
139 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
140 [assignment: *list of security attributes*]
141 [assignment: *the authorised identified roles*]
142 [assignment: *access control SFP(s), information flow control SFP(s)*]
143 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
144 [assignment: *list of security attributes*]
145 [assignment: *the authorised identified roles*]
146 [assignment: *access control SFP(s), information flow control SFP(s)*]
147 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
148 [assignment: *the authorised identified roles*]
149 [assignment: *access control SFP(s), information flow control SFP(s)*]
150 [selection: *change_default, query, modify, delete, [assignment: other operations]*]
151 [assignment: *the authorised identified roles*]
152 [assignment: *access control SFP(s), information flow control SFP(s)*]
153 [selection: *change_default, query, modify, delete, [assignment: other operations*]]
154 [assignment: *list of security attributes*]
155 [assignment: *the authorised identified roles*]

Application Note 30

According to (6) the SSA can query the Signer attributes listed in FIA_USB.1 but those are not security relevant. The Signer PIN and private key cannot be queried, only the Signer have access to those.

FMT_MSA.1/Privileged User	Management of security attributes
FMT_MSA.1.1/	Privileged User The TSF shall enforce the *(1) Privileged User Creation SFP*[156] to restrict the ability to *create and query*[157] the security attributes *listed in FIA_USB.1 for Privileged User*[158] to *authorised Privileged User*[159].

FMT_MSA.2	Secure security attributes
FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for *all security attributes listed in FIA_USB.1*[160]

FMT_MSA.3/Signer	Static attribute initialization
FMT_MSA.3.1/Signer	The TSF shall enforce the *Signer Creation SFP*[161] to provide *restrictive*[162] default Signer values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/Signer	The TSF shall allow the *Privileged User*[163] to specify alternative initial values to Signer override the default values when an object or information is created.

FMT_MSA.3/Privileged User	Static attribute initialisation
FMT_MSA.3.1/Privileged User	The TSF shall enforce the *Privileged User Creation SFP*[164] to provide *restrictive*[165] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/Privileged User	The TSF shall allow the *Privileged User*[166] to specify alternative initial values to override the default values when an object or information is created.

Application Note 31

This SFR doesn't apply as there are no security attributes stored for Privileged User other than public key or passwords and there are no default values for that.

[156] [assignment: *access control SFP(s), information flow control SFP(s)*]
[157] [selection: *change_default, query, modify, delete, [assignment: other operations*]]
[158] [assignment: *list of security attributes*]
[159] [assignment: *the authorised identified roles*]
[160] [assignment: *list of security attributes*]
[161] [assignment: *access control SFP, information flow control SFP*]
[162] [selection, choose one of: *restrictive, permissive, [assignment: other property*]]
[163] [assignment: *the authorised identified roles*]
[164] [assignment: access control SFP, information flow control SFP]
[165] [selection, choose one of: *restrictive, permissive, [assignment: other property*]]
[166] [assignment: *the authorised identified roles*]

FMT_MTD.1	Management of TSF data
FMT_MTD.1.1	The TSF shall restrict the ability to *modify*[167] the *R.TSF_DATA*[168] data to *Privileged User*[169].

FMT_SMF.1	Specification of Management Functions
FMT_SMF.1.	The TSF shall be capable of performing the following management functions: *(1) Signer management,* *(2) Privileged User management,* *(3) Configuration management,* *(4) None*[170].

FMT_SMR.2	Restrictions on security roles
FMT_SMR.2.1	The TSF shall maintain the roles: *Signer and Privileged User* **(Admin and IDP)**, *none*[171].
FMT_SMR.2.2	The TSF shall be able to associate users with roles.
FMT_SMR.2.3	The TSF shall ensure that the conditions *Signer can't be a Privileged User*[172] are satisfied.

Application Note 32

The restriction on the security roles are explained in section 7.5

6.4.6 Protection of TSF (FPT)

FPT_PHP.1	Passive
FPT_PHP.1.1	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3	Resistance
FPT_PHP.3.1	The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices/elements*] by responding automatically such that the SFRs are always enforced.

[167] [selection: *change_default, query, modify, delete, clear, [assignment: other operations*]]
[168] [assignment: *list of TSF data*]
[169] [assignment: *the authorised identified roles*]
[170] [assignment: *list of management functions to be provided by the TSF*]
[171] **[assignment: *the other authorised identified roles*]**
[172] **[assignment: *conditions for the different roles*]**

Application Note 33

The TOE is implemented as a local application within the same physical boundary as the cryptographic module defined in [EN 419221-5]. The SFRs FTP_PHP.* rely on the similar SFRs described in the ST for the cryptographic module [HSM_ST]. This means that the TOE always generates keypairs in the certified CM. All cryptographic operations are performed within and by the certified CM.

FPT_RPL.1	Replay detection
FPT_RPL.1.1	The TSF shall detect replay for the following entities: *R.SAD*[173].
FPT_RPL.1.2	The TSF shall perform *reject the signature operation*[174] when replay is detected.

FPT_STM.1	Reliable time stamps
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

Application Note 34

The TOE is able to provide reliable time stamps as it uses the certified Thales Luna K7 for time source.

FPT_TDC.1	Inter-TSF basic TSF data consistency
FPT_TDC.1.1	The TSF shall provide the capability to consistently interpret *(1) R.Signer,* *(2) R.Reference_Signer_Authentication_Data,* *(3) R.SAD,* *(4) R.DTBS/R* *(5) R.SVD* *(6) R.Privileged_User* *(7) R.Reference_Privileged_User_Authentication_Data* *(8) R.TSF_DATA*[175] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2	The TSF shall use *data integrity either on data or on communication channel*[176] when interpreting the TSF data from another trusted IT product.

6.4.7 Trusted Paths/Channels (FTP)

FTP_TRP.1/SSA	Inter-TSF Trusted path

[173] **[assignment: *list of identified entities*]**
[174] **[assignment: *list of specific actions*]**
[175] [assignment: *list of TSF data types*]
[176] [assignment: *list of interpretation rules to be applied by the TSF*]

FTP_TRP.1.1/SSA	The TSF shall provide a communication path between itself and *Privileged User(IDP) through SSA*[177] 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*[178].
FTP_TRP.1.2/SSA	The TSF shall permit *Privileged User through SSA*[179] to initiate communication via the trusted path.
FTP_TRP.1.3/SSA	The TSF shall require the use of the trusted path for *(1) FDP_ACC.1.1/Privileged User Creation* *(2) FDP_ACC.1/Signer Creation* *(3) FDP_ACC.1/Signer Maintenance* *(4) FDP_ACC.1/Signer Key Pair Generation* *(5) FDP_ACC.1/Signer Key Pair Deletion* *(6) FDP_ACC.1/Supply DTBS/R* *(7) FDP_ACC.1/TOE Maintenance* *(8) none*[180].

FTP_TRP.1/SIC	Inter-TSF Trusted path

FTP_TRP.1.1/SIC	The TSF shall provide a communication path between itself and the *Remote Signer through the SIC*[181] 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*[182].
FTP_TRP.1.2/SIC	The TSF shall permit the *Remote Signer through SIC*[183] to initiate communication via the trusted path.
FTP_TRP.1.3/SIC	The TSF shall require the use of the trusted path for *(1) FDP_ACC.1/Signer Maintenance* *(2) FDP_ACC.1/Signer Key Pair Generation* *(3) FDP_ACC.1/Signer Key Pair Deletion* *(4) FDP_ACC.1/Signing* *(5) [assignment: other services for which a trusted path is required]*[184].

Application Note 35

The TOE does not verify the SIC as a physical communication end point but it uses end to end encryption between itself and the Signer so it can be considered separate channel.

FTP_ITC.1/CM Inter-TSF trusted channel

[177] [selection: *remote, local*]
[178] [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]
[179] [selection: *the TSF, local users, remote users*]
[180] [selection: *initial user authentication, [assignment: other services for which trusted path is required]*]
[181] [selection: *remote, local*]
[182] [selection: *modification, disclosure, [assignment: other types of integrity or confidentiality violation]*]
[183] [selection: *the TSF, local users, remote users*]
[184] **[selection: *initial user authentication, [assignment: other services for which trusted path is required]*]**

FTP_ITC.1.1/CM The TSF shall provide a communication path between itself and a cryptographic module certified according to [EN 419221-5][185] that is logically distinct from other communication paths and provides assured authentication of its end points and protection of the communicated data from modification or disclosure.

FTP_ITC.1.2/CM The TSF shall permit the TSF and a cryptographic module certified according to [EN 419221-5][186] to initiate communication via the trusted channel.

FTP_ITC.1.3/CM The TSF shall initiate communication via the trusted channel for *all communication between itself and the HSM*.

6.5 Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with AVA_VAN.5. The assurance components are identified in the table below with the augmented item in bold.

Since the TOE is operated in a physically protected environment as described in OE.ENV an evaluation against this ST will probably not include physical attacks.

Assurance Class	Assurance Components
Development (ADV)	Security architecture description (ADV_ARC.1)
	Complete functional specification (ADV_FSP.4)
	Implementation representation of the TSF (ADV_IMP.1)
	Basic modular design (ADV_TDS.3)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life-cycle support (ALC)	Production support, acceptance procedures and automation (ALC_CMC.4)
	Problem tracking CM coverage (ALC_CMS.4)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Well-defined development tools (ALC_TAT.1)
Security Target evaluation (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)

[185] another trusted IT product

[186] **[selection:** ***the TSF, another trusted IT product*****]**

	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.2)
	Derived security requirements (ASE_REQ.2)
	Security problem definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Tests (ATE)	Analysis of coverage (ATE_COV.2)
	Testing: basic design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing - sample (ATE_IND.2)
Vulnerability assessment (AVA)	Advanced methodical vulnerability analysis (AVA_VAN.5)

Table11: Assurance class and components

7 TOE Summary Specification

The TOE employs a variety of security functionality (TSF) to satisfy the SFRs in order to provide the creation of digital signatures. This chapter summarizes the security capabilities of the TOE to clarify the solutions implemented to ensure that the SFRs are satisfied.

Each of the following sections describes the security functionality related to one of the SFR classes identified in Chapter 6. The sections are when relevant ordered by the functionality provided.

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

1. Security Audit
2. Cryptographic Support
3. User Data Protection
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. Trusted Path/Channels

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

7.1 Security Audit (FAU)

The TSF is responsible for the generation and content of the log entries, but the logging itself happens in the HSM. Practically, the TOE generates logs for the performed operations and forwards them to the HSM. Each log entry indicates what event occurred when, and who initiated it. Critical events are logged automatically.The TOE invokes the Thales Luna K7 Cryptographic Module audit services via internal API calls. The CM is [EN 419221-5] certified and has the same (or even higher) audit

requirements as [EN 419241-2]. As all the cryptographic operations are performed in the Thales Luna K7 Cryptographic Module, the logs of these operations are automatically managed by the CM.

The HSM stores a record of past operations that is suitable for security audit review. Audit logging sends HSM log event records to a secure database on the local file system, with cryptographic safeguards ensuring verifiability, continuity, and reliability of HSM event log files.

The logs entries are stored outside of the TOE logical boundaries.

Relevant SFRs: FAU_GEN.1, FAU_GEN.2

7.2 Cryptographic Support (FCS)

The TOE is installed locally on Thales Luna K7 Cryptographic Module and has access to the CM crypto library via local API calls. The CM is [EN 419221-5] certified and fulfils all cryptographic requirements including random number generation. Whenever there is a request coming from the SCA it is processed in the SAM and after the authorization of the request the actual crypto operation is being forwarded to the CM crypto module. All cryptographic operations are initiated by the TOE, but the operations are fully executed in and by the certified Thales Luna K7 Cryptographic Module.

The TOE supports the following cryptographic operations:

- Generation of RSA, ECDSA and AES keys
- Creation and verification of digital signatures with RSA and ECDSA keys
- Encryption and Decryption of data with RSA, AES CBC
- Message Digest using SHA1, SHA256, SHA384, SHA512 algorithms

After the signing key is generated by the CM, it is encrypted and exported by the TOE to an external database managed by SSA. The encrypted key deletion from the external database is not managed by the TOE. The encrypted signing keys are loaded to the HSM by the TOE right before every signing operation. The signing operation is done in the CM. The keys are deleted automatically from the HSM right after the signature is created.

Relevant SFRs: FCS_CKM.1/AES, FCS_CKM.1/RSA, FCS_CKM.1/ECC, FCS_CKM.4, FCS_COP.1/Encrypt and Decrypt, FCS_COP.1/Message digest, FCS_COP.1/Sign and Verify, FCS_RNG.1

7.3 User Data Protection (FDP)

The TOE protects each user's data. The roles of the TOE are as follows:

Privileged Users (IDPs and Admins) and Signers.

The Privileged Users are created during the TOE setup/configuration. During setup, each Administrator must enter their PIN codes and passwords on the NSSAM Admin Console. Those PINS and passwords will be stored on NSSAM secure filesystem and cannot be changed after this point.

Privileged Users (IDP) can be created by Privileged Users (Admins) only after they are authorized by the TOE verifying their passwords. When IDPs are registered the relevant IDP data (name, issuerClaim and public key) will be stored in the TOE secure filesystem.

Relevant SFRs: FDP_ACC.1/Privileged User Creation, FDP_ACF.1/Privileged User Creation

Signers can be created by IDPs only. Admin cannot create any Signers nor Signers can create other Signers. The only maintenance that can be done with the Signers is blocking their signing key in case they provide a wrong PIN.

Key generation is available only for the Privileged User (IDP). For the key generation, the Signer provides PIN which will be used to authorize them to create digital signatures.

Authorization Data of the Signer is managed by the SCA and confirmed by the IDP. The IDP signature is verified before processing the request of the SCA. The Signers provide their PIN during key generation which is used to create the key authorization data for their signing key. Also, they provide the PIN during signature creation and if the key authorization data (that includes the PIN) does not match, the key cannot be authorized and used for signing.

The signing keys are encrypted with multiple infrastructure keys (two SKS passwords and the SKS Master key). The encrypted keys are then exported and stored in an external database. Before every signature is created with the key it must be imported back to the HSM where it can be decrypted and used for signing. After the signature operation, it is removed from the HSM memory and never leaves it in decrypted format.

Signer keys are loaded into the TOE before every signing operation, being decrypted only for the signing operation and deleted right after the signature is created automatically from the HSM. Before the signature, the keys have to be authorized inside the HSM with the very same key authorization data that contains the same PIN that was provided during key generation.

Relevant SFRs: FDP_ACC.1/Signer Creation, FDP_ACF.1/Signer Creation, FDP_ACC.1/Signer Maintenance, FDP_ACF.1/Signer Maintenance, FDP_ACC.1/Signer Key Pair Generation, FDP_ACF.1/Signer Key Pair Generation, FDP_ACC.1/Signer Key Pair Deletion, FDP_ACF.1/Signer Key Pair Deletion

The TOE does not provide facilities to supply the DTBS/R(s) but it signs the DTBS/R the SSA provided.

The Signer sends their authentication data via the SCA. The JWT is signed by the IDP. The TOE verifies the IDP signature and if it’s valid and not expired. The Signer also sends the PIN. All data is encrypted with a session key generated in the Crypto Module. The data is sent to the Crypto Module along with the encrypted signing key, which is then decrypted by the use of the SMK key and the 2 SKS Admin Passwords, and authorized for use by the key authorization data. If any of the given keys, or passwords, or PIN doesn’t match, the key cannot be used.

Relevant SFRs: FDP_ACC.1/Supply DTBS/R, FDP_ACF.1/Supply DTBS/R, FDP_ACC.1/Signing, FDP_ACF.1/Signing

The TOE configuration is done using NSSAM Admin Console component that is available only for Admins. During the TOE setup Admin needs to provide their Security Officer and Limited Security Officer passwords to be able to communicate with the HSM. Also, they need to provide multiple passwords and PINs to be used for key encryption and session encryption. After setting up the TOE there are only a couple of management functions available:

- PIN complexity setting (complex or basic)
- PIN minimum length
- RSA Key size
- Default EC curve

- Register IDP
- Delete register IDP
- Change time drift
- Add NSSAM license
- Create license request
- Backup NSSAM Master RSA
- Restore NSSAM Master RSA
- Show configured NSSAM policies
- List registered IDP
- Configure max user sessions
- Configure SHA1 usage
- Delete specific user session keys
- Delete all user session keys
- List locked keys
- Delete specific locked key
- Delete specific user key
- Delete all user keys
- Export Master RSA Public key

Importing configuration is for backup purposes. The exported configuration can only be restored on the same HSM partition that it was exported from and requires each admin passwords to be entered during the restore process.

All other changes in the configuration require NSSAM reset from the very beginning.

There is no Signer data stored in the TOE so nothing can be exported. The signer's key pair along with its attributes are sent back to the TSP database in an encrypted blob. Signer objects are imported in the TOE right before the signature creation and then removed immediately when the signature is complete.

There is no privileged user data that could be exported or imported only the configuration data that was mentioned above, and that data is always encrypted.

The Signer's signing keys are imported to the TOE and decrypted in the HSM only before the Signature operation.

During transformation, the data is protected for confidentiality and integrity. The requests contain a JWT token that is signed by the IDP. On top of that, all parameters are encrypted with AES encryption that can be decrypted only inside the TOE.

Relevant SFRs: FDP_ACC.1/TOE Maintenance, FDP_ACF.1/TOE Maintenance, FDP_ETC.2/Signer, FDP_IFC.1/Signer, FDP_IFF.1/Signer, FDP_ETC.2/Privileged User, FDP_IFC.1/Privileged User, FDP_IFF.1/Privileged User, FDP_ITC.2/Signer, FDP_ITC.2/Privileged User, FDP_UCT.1, FDP_UIT.1

7.4 Identification and Authentication (FIA)

Every user is identified before they are allowed to perform any action in the TOE. Different roles have different authentication methods.

For Signer and SCA an external Identity Provider shall be configured that identifies and authenticates the Signer. After they are authenticated the IDP signs the request coming from the SCA. The IDP signature is verified by the TOE before processing the request.

In addition to that, Signers provide PIN during the key generation that will be used as a part of the Signer authentication data, and a part of the key authorization data for their private keys. In the case of creating a digital signature, the Signer's PIN is also needed and without that, the signing key cannot be authorized and used for signature. If the request is signed by the IDP but the PIN is wrong the TOE counts the failed attempts and after 3 attempts, it suspends the relevant signing key. When a key authorization is failed it will be kept in the HSM and remains blocked until a good PIN is provided by the Signer and valid key authorization data is formed. If the failed attempt counter reaches 3, the key becomes inaccessible. The inaccessible keys can be deleted from the HSM manually by the Admins.

Privileged Users (Admins) are provided by Thales Luna K7. The Crypto Officer (CO) role is required to set up the TOE, Limited Crypto Officer (LCO) role is required to operate the TOE so whenever the TOE needs CM features, they need to provide passwords of either CO or LCO.

The only operation that is available without authentication is the initialize command which is the very first step of the TOE setup and is not available in the operation state.

Relevant SFRs: FIA_AFL.1, FIA_ATD.1, FIA_UAU.1, FIA_UAU.5/Signer, FIA_UAU.5/Privileged User, FIA_UID.2, FIA_USB.1

7.5 Security Management (FMT)

Every data of the Signer is managed outside the TOE. The only security-relevant data is the private key that is encrypted with TOE infrastructural keys and the Signer's PIN is needed to be authorized for signing. When it's loaded to the TOE and decrypted in the HSM it is deleted automatically after the successful signature. If the authorization failed due to a wrong PIN, only Admins can delete it from the HSM. Signer can delete the key if they provide a good PIN so the signature is successful and the key is deleted automatically after that.

The key pair generation is invoked by the SCA in the name of the Signer which provides their PIN.

Only authorised Admins can register new Identity Providers.

Only authorised Admins can manage the TSF data. Signers have no access to management functions. Only Admins have access to the NSSAM Admin Console that provides configuration functionalities.

The TOE manages the following roles:

- Signer – Individuals who have their signing keys managed by the TOE. They access the TOE via Using SCAs. They don't have access to any management/configuration functions they have access to only their key and are able to perform digital signatures.
- Privileged User – Users with privileges. They configure and manage the TOE and their users but don't have access to the Signer's keys. They do not perform digital signatures.
    - IDP – Identity Provider that signs JWT token coming from the SCA. They have access to the TOE via the NSSAM Driver component. All requests they sign are coming from the Signer themselves so there is no single request from the IDP. It's always just a signature on the Signer's JWT token.
    - Admin – People who manage the TOE. There are different types of Admins

- Thales Crypto Officer (CO) – Provided by the Thales Luna K7. Used for the configuration of the HSM and installing/configuring the TOE on the HSM. Used only in the configuration phase. It has access to the TOE via NSSAM Admin Console component.
- Thales Limited Crypto Officer (LCO) – Provided by Thales Luna K7. Used to perform operational commands on the HSM invoked by the TOE[187].

The Signer's PIN shall match the required PIN length (configurable 6-32) and format (upper case, lower case, number and special character shall be used) defined by Admins.

Relevant SFRs: FMT_MSA.1/Signer, FMT_MSA.1/Privileged User, FMT_MSA.2, FMT_MSA.3/Signer, FMT_MSA.3/Privileged User, FMT_MTD.1, FMT_SMF.1, FMT_SMR.2

7.6 Protection of the TSF (FPT)

The TOE is installed as an FM (functional module) on the Thales Luna K7 within the same physical enclosure meaning it has the very same physical protection against passive and active detection of tamper.

All requests contain a JWT token which is signed by a registered IDP. This guarantees the integrity protection of the request so the signature operation cannot be repeated with overwriting the previous request. All start session responses are signed with the NSSAM RSA Master key. Other requests are encrypted with a unique session key (for that session) which can be used only once (one operation, successful or not)

The TOE is able to provide reliable time stamps as it uses the certified HSM Thales Luna K7 for time source.

The Data stored outside the TOE (signing keys) are stored encrypted. If someone tries overwriting it, it will not be decryptable inside the HSM anymore. In addition to that without knowing the key's PIN (that is not stored anywhere) the key cannot be used to create signatures.

Relevant SFRs: FPT_PHP.1, FPT_PHP.3, FPT_RPL.1, FPT_STM.1, FPT_TDC.1

7.7 Trusted Paths/Channels (FTP)

For communication with all external SCA the TOE uses a secure channel identified as a Secure Trusted Channel (STC) which provides authentication of its end-points and protection of confidentiality and integrity of data sent over the channel. This STC solution was implemented by Thales and this is the same method that protects the Thales Luna K7 communication channels.

On the top of STC the TOE uses an additional AES encryption between itself and the SCAs.

Channel security is used between the following entities:

- SCA and the NSSAM Driver (TLS + AES)
- NSSAM Driver and the TOE (STC or NTLS (configurable) + AES)
- TOE and the HSM (STC)

[187] CO and LCO are HSM roles, but their passwords needs to be given by the TOE Administrators using the NSSAM Admin Console. Whenever a command is entered on the NSSAM Admin Console, the TOE validates the passwords with the HSM so CO and LCO are both considered HSM and TOE roles.

Relevant SFRs: FTP_TRP.1/SSA, FTP_TRP.1/SIC, FTP_ITC.1/CM

8 Rationale

8.1 Security Requirements Rationale

8.1.1 Security Requirements Coverage

The following table is used to demonstrate that every SFR is used to cover an objective and that every objective is covered by an SFR. The table is not complete in the sense that all possible crosses are created.

	OT.SIGNER_PROTECTION	OT.REFERENCE_SIGNER_AUTHENTICATION_DATA	OT.SIGNER_KEY-PAIR-GENERATION	OT.SVD	OT.PRIVILEGED_USER_MANAGEMENT	OT.PRIVILEGED_USER_AITHENTICATION	OT.PRIVILEGED_USER_PROTECTION	OT.SIGNER_MANAGEMENT	OT.SYSTEM_PROTECTION	OT.AUDIT_PROTECTION	OT.SAD_VERIFICATION	OT.SAP	OT.SIGNATURE.AUTHENTICATION_DATA_PROTECTION	OT.DTBSR_INTEGRITY	OT.SIGNATURE_INTEGRITY	OT.CRYPTO	OT.RANDOM
Security Audit																	
FAU_GEN.1										X							
FAU_GEN.2										X							
Cryptographic Support																	
FCS_CKM.1/*			X													X	
FCS_CKM.4			X														
FCS_COP.1/*			X												X	X	
FCS_RNG.1			X														X
User Data Protection																	
FDP_ACC.1/ Privileged User Creation					X												

FDP_ACF.1/ Privileged User Creation				X												
FDP_ACC.1/ Signer	X						X									
Creation																
FDP_ACF.1/ Signer Creation	X						X									
FDP_ACC.1/ Signer Maintenance	X															
FDP_ACF.1/ Signer Maintenance	X															
FDP_ACC.1/ Signer Key Pair Generation		X	X													
FDP_ACF.1/ Signer Key Pair Generation		X	X													
FDP_ACC.1/ Signer Key Pair Deletion							X									
FDP_ACF.1/ Signer Key Pair Deletion							X									
FDP_ACC.1/ Supply DTBS/R													X			
FDP_ACF.1/ Supply DTBS/R													X			
FDP_ACC.1/										X				X		
Signing																
FDP_ACF.1/ Signing										X				X		
FDP_ACC.1/								X								

TOE Maintenance																	
FDP_ACF.1/TOE Maintenance									X								
FDP_ETC.2/ Signer	X																
FDP_IFC.1/Signer	X																
FDP_IFF.1/Signer	X																
FDP_ETC.2/ Privileged User					X		X										
FDP_IFC.1/Privileged User					X		X										
FDP_IFF.1/privileged User					X		X										
FDP_ITC.2/Signer	X																
FDP_ITC.2/Privileged User					X		X										
FDP_UCT.1	X																
FDP_UIT.1	X																
Identification and Authentication																	
FIA_AFL.1						X					X						
FIA_ATD.1	X				X		X										
FIA_UAU.1						X					X						
FIA_UAU.5/Signer											X						
FIA_UAU.5/Privileged User						X											
FIA_UID.2					X		X	X									
FIA_USB.1	X		X		X		X										
Security Management																	

FMT_MSA.1/ Signer								X									
FMT_MSA.1/ Privileged User					X			X									
FMT_MSA.2					X			X									
FMT_MSA.3/ Signer								X									
FMT_MSA.3/ Privileged User					X			X									
FMT_MTD.1									X								
FMT_SMF.1									X								
FMT_SMR.2									X								
Protection of the TSF																	
FPT_PHP.1									X								
FPT_PHP.3									X								
FPT_RPL.1												X					
FPT_STM.1										X							
FPT_TDC.1	X				X												
Trusted Path/Channels																	
FTP_TRP.1/SSA									X					X			
FTP_TRP.1/SIC												X	X	X			
FTP_ITC.1/CM			X												X		

Table12: SFR Coverage

OT.SIGNER_PROTECTION is handled by requirements export and import of R.Signer in a secure way. (FDP_ETC.2/Signer, FDP_IFC.1/Signer, FDP_IFF.1/Signer, FDP_ITC.2/Signer, FDP_UCT.1 FDP_UIT.1 and FPT_TDC.1). The actual description of the data is described in FIA_ATD.1 and FIA_USB.1.

OT.REFERENCE_SIGNER_AUTHENTICATION_DATA is handled by FDP_ACC.1/Signer Creation, FDP_ACF.1/Signer Creation, FDP_ACC.1/Signer Maintenance and FDP_ACF.1/Signer Maintenance

which describes access control for creating and updating R.Signer and R.Reference_Signer_Authenticaton_Data.

OT.SIGNER_KEY_PAIR_GENERATION is handled by the requirements for key generation and cryptographic algorithms in FCS_CKM.1/* and FCS_COP.1/*. FCS_RNG.1 provides a random source for key generation. FCS_CKM.4 describes the requirements for key destruction. FDP_ACC.1/Signer Key Pair Generation and FDP_ACF.1/Signer Key Pair Generation describes access control for creating a key pair. FIA_USB.1 describes that R.Signing_Key_Id is associated with Signer. FTP_ITC.1/CM can be used to communicate securely with a Cryptographic Module.

OT.SVD is handled by the requirements in FDP_ACC.1/Signer Key Pair Generation and FDP_ACF.1/Signer Key Pair Generation.

OT.PRIVILEGED_USER_MANAGEMENT is handled by requirements for export and import of R.Privileged User in a secure way (FDP_ETC.2/Privileged User, FDP_IFC.1/Privileged User, FDP_IFF.1/privileged User, FDP_ITC.2/Privileged User and FPT_TDC.1). The actual description of the data is described in FIA_ATD.1 and FIA_USB.1. Authentication of Privileged User is handled by FIA_UID.2, FMT_MSA.1/Privileged User, FMT_MSA.2 and FMT_MSA.3/Privileged User. FDP_ACC.1/Privileged User Creation and FDP_ACF.1/Privileged User Creation describes access controls for creating Privileged Users.

OT.PRIVILEGED_USER_AUTHENTICATION is handled by FIA_AFL.1, FIA_UAU.1 and FIA_UAU.5/Privileged User.

OT.PRIVILEGED_USER_MANAGEMENT is handled by requirements for export and import of R.Privileged User in a secure way (FDP_ETC.2/Privileged User, FDP_IFC.1/Privileged User, FDP_IFF.1/privileged User, FDP_ITC.2/Privileged User and FPT_TDC.1). The actual description of the data is described in FIA_ATD.1 and FIA_USB.1. Authentication of Privileged User is handled by FIA_UID.2, FMT_MSA.1/Privileged User, FMT_MSA.2 and FMT_MSA.3/Privileged User. FDP_ACC.1/Privileged User Creation and FDP_ACF.1/Privileged User Creation describes access controls for creating Privileged Users.

OT.SIGNER_MANAGEMENT is handled by the requirements for access control in FDP_ACC.1/Signer Creation, FDP_ACF.1/Signer Creation, FDP_ACC.1/Signer Maintenance and FDP_ACF.1/Signer

Maintenance. Authentication of Signers and Privileged Users are handled by FIA_UID.2, FMT_MSA.1/Signer, FMT_MSA.1/Privileged User, FMT_MSA.2, FMT_MSA.3/Signer and FMT_MSA.3/Privileged User.

OT.SYSTEM_PROTECTION is handled by FMT_MTD.1, FMT_SMF.1 and FMT_SMR.2. FDP_ACC.1/TOE Maintenance and FDP_ACF.1/TOE Maintenance describes access control rules for managing TSF data.

FPT_PHP.1 and FPT_PHP.3 describes requirements for TSF protection. FTP_TRP.1/SSA describes that only a Privileged User can maintain the TOE.

OT.AUDIT_PROTECTION is handled by the requirements for audit record generation FAU_GEN.1 and FAU_GEN.2 using reliable time stamps in FPT_STM.1.

OT.SAD_VERIFICATION is handled by the FIA_AFL.1, FIA_UAU.1 and FIA_UAU.5/Signer. FDP_ACC.1/Signing and FDP_ACF.1/Signing describes access control rules for the signature operation and well as for SAP verification.

OT.SAP is covered by the requirements FTP_TRP.1/SIC and FPT_RPL.1 the protocol between the SIC and TSF.

OT.SIGNATURE_AUTHENTICATION_DATA_PROTECTION is covered by FTP_TRP.1/SIC, which describes the requirements for data transmitted to the TOE, is protected in integrity.

OT.DTBSR_INTEGRITY is covered by FTP_TRP.1/SSA and FTP_TRP.1/SIC requiring data transmission to be protected in integrity.

OT.SIGNATURE_INTEGRITY is handled by FCS_COP.1/*, which describes requirements on the algorithms. FTP_ITC.1/CM may be used to transmit data securely between the TOE and the Cryptographic Module. Access control for the signature operation is ensured by FDP_ACC.1/Signing and FDP_ACF.1/Signing.

OT.CRYPTO is covered by FCS_CKM.1/* and FCS_COP.1/*, which describes requirements for key generation and algorithms.

OT.RANDOM is handled by FCS_RNG.1, which describes requirement on the random number generation.

8.2 SFR Dependencies

The dependencies between SFRs are addressed as shown in the table below

Requirement	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 and FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1
FCS_RNG.1	None	No dependents
FDP_ACC.1/Privileged User Creation	FDP_ACF.1	FDP_ACF.1/Privileged User Creation
FDP_ACC.1/Signer Creation	FDP_ACF.1	FDP_ACF.1/Signer Creation

FDP_ACC.1/Signer Maintenance	FDP_ACF.1	FDP_ACF.1/Signer Maintenance
FDP_ACC.1/Signer Key Pair Generation	FDP_ACF.1	FDP_ACF.1/Signer Key Pair Generation
FDP_ACC.1/Signer Key Pair Deletion	FDP_ACF.1	FDP_ACF.1/Signer Key Pair Deletion
FDP_ACC.1/Supply DTBS/R	FDP_ACF.1	FDP_ACF.1/Supply DTBS/R
FDP_ACC.1/Signing	FDP_ACF.1	FDP_ACF.1/Signing
FDP_ACC.1/TOE Maintenance	FDP_ACF.1	FDP_ACF.1/TOE Maintenance
FDP_ACF.1/Privileged User Creation	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Privileged User Creation FMT_MSA.3/Privileged User
FDP_ACF.1/Signer Creation	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Creation FMT_MSA.3/Signer
FDP_ACF.1/Signer Maintenance	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Maintenance FMT_MSA.3/Signer
FDP_ACF.1/Signer Key Pair Generation	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Key Pair Generation FMT_MSA.3/Signer
FDP_ACF.1/Signer Key Pair Deletion	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signer Key Pair Deletion FMT_MSA.3/Signer
FDP_ACF.1/Supply DTBS/R	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Supply DTBS/R FMT_MSA.3/Signer
FDP_ACF.1/Signing	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Signing FMT_MSA.3/Signer
FDP_ACF.1/TOE Maintenance	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/TOE Maintenance FMT_MSA.3/Privileged User
FDP_ETC.2/Signer	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/Signer
FDP_ETC.2/Privileged User	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/Privileged User
FDP_IFC.1/Signer	FDP_IFF.1	FDP_IFF.1/Signer
FDP_IFF.1/Signer	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Signer FMT_MSA.3/Signer
FDP_IFC.1/Privileged User	FDP_IFF.1	FDP_IFF.1/Privileged User
FDP_IFF.1/Privileged User	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Privileged User FMT_MSA.3/Privileged User
FDP_ITC.2/Signer	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FTP_TDC.1	FDP_IFC.1/Signer FTP_TRP.1/SSA and FTP_TRP.1/SIC FPT_TDC.1
FDP_ITC.2/Privileged User	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FDP_IFC.1/Privileged User FTP_TRP.1/SSA

	FTP_TDC.1	FPT_TDC.1
FDP_UCT.1	[FTP_ITC.1 or FTP_TRP.1] [FDP_ACC.1 or FDP_IFC.1]	FTP_TRP.1/SSA and FTP_TRP.1/SIC FDP_IFC.1/Signer FDP_IFC.1/Privileged User
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FDP_IFC.1/Signer FDP_IFC.1/Privileged User FTP_TRP.1/SSA and FTP_TRP.1/SIC
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.5/Signer	None	
FIA_UAU.5/Privileged User	None	
FIA_UID.2	None	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MSA.1/Signer	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1/Signer FMT_SMR.2 FMT_SMF.1
FMT_MSA.1/Privileged User	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1/Privileged User FMT_SMR.2 FMT_SMF.1
FMT_MSA.2	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	FDP_IFC.1/Signer FDP_IFC.1/Privileged User FMT_MSA.1/Signer FMT_MSA.1/Privileged User FMT_SMR.2
FMT_MSA.3/Signer	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Signer FMT_SMR.2
FMT_MSA.3/Privileged User	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Privileged User FMT_SMR.2
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 FMT_SMF.1
FMT_SMF.1	None	
FMT_SMR.2	FIA_UID.1	FIA_UID.2
FPT_PHP.1	None	
FPT_PHP.3	None	
FPT_RPL.1	None	
FPT_STM.1	None	
FPT_TDC.1	None	
FTP_TRP.1/SSA	None	

FTP_TRP.1/SIC	None
FTP_ITC.1/CM	None

Table13: SFR Dependences

8.2.1 Rationales for SARs

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, through rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

As the TOE manages signature creation data generation and authorises the use, it manages security attributes that can only be ensured by the TOE. While the TOE is assumed to be in a physically protected environment, it is still subject to logical remote attacks and should be evaluated to deal with High attack potential.

EAL4 is therefore augmented with AVA_VAN.5.

Abbreviations

AC	Access Control
AES	Advanced Encryption Standard
API	Application Programming Interface
AS	Authentication System
CA	Certification Authority
CC	Common Criteria, ISO/IEC 15408, Evaluation criteria for IT security
CM	Cryptography Module certified according to prEN 419221-5:2016
CSR	Certificate Signing Request
Certificate	Certificate for electronic signature as defined in eIDAS article 3.
DTBS/R	Data To Be Signed Representation
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
HSM	Hardware Security Module
IDP	Identity Provider
KEK	Key Encryption Key
OTP	One-Time Password
RDBMS	Relational database management system

SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SCA	Signature Creation Application
SIC	Signer's Interaction Component
SSA	Server Signing Application, in this case the TSP backend service
SVD	Signature Verification Data
ST	Security Target
TOE	Target of Evaluation
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing
QSCD	Qualified Electronic Signature (or Electronic Seal) Creation Device as defined in the eIDAS Regulation [8]

Bibliography

[eIDAS]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[Assurance]	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model; Version 3.1, Revision 5. CCMB-2017-04001, April 2017.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 5. CCMB-2017-04002, April 2017.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 5. CCMB-2017-04003, April 2017.
[EN 419241-1]	Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements, EN 419241-1:2018, July 2018
[EN 419241-2]	Trustworthy Systems Supporting Server Signing - Part 2: Protection Profile for QSCD for Server Signing, EN 419241-2:2019, February 2019
[EN 419221-5]	Protection Profiles for Trust Service Provider Cryptographic Modules - Part 5: Cryptographic Module for Trust Services, EN 419221-5:2018, May 2018

[ETSI EN 319 411-1]	ETSI, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. 2016.
[FIPS 180-4]	Federal Information Processing Standards Publication 180-4, Secure Hash Standard (SHS), NIST, August 2015.
[FIPS 186-4]	FIPS PUB 186-4, Digital Signature Standard (DSS) / National Institute of Standards and Technology (NIST), USA, July 2013
[FIPS 186-5]	National Institute of Standards and Technology (2023) Digital Signature Standard (DSS). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 186-5
[FIPS 197]	National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 197-upd1, updated May 9, 2023.
[PKCS#1]	RSA Laboratories, PKCS #1: RSA Encryption Standard, Version v2.2
[HSM_ST]	Thales Luna K7 Cryptographic Module Security Target, 6th May 2022
[Guidance]	Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM Operations Guide, version 1.4 Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM Installation Guide, version 1.4 Nextsense Remote QSCD Signature Activation Module (SAM) 3.4 for Thales® Luna HSM Installation Prerequisites, version 1.4