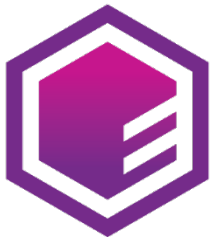

Entrust E.U.

Security Target

Cryptographic Security Platform (CSP)

September 25, 2025

Contents

1 Security Target introduction

1.1 Security Target and TOE Reference

Title and version	**Security Target – Cryptographic Security Platform (CSP), version 1.8.**
Issue data	September 2025.
Author	Entrust E.U.
CC version	Common Criteria 2022 Release 1.
Evaluated TOE	Cryptographic Security Platform (CSP) | PKI Hub, version 1.2.
TOE commercial name	Cryptographic Security Platform (CSP), version 1.2.

1.2 TOE Overview

This section briefly describes the usage of the TOE and its major security features, identifies the TOE type and identifies any major non-TOE hardware/software/firmware required by the TOE.

1.2.1 Usage and major security features of the TOE

The TOE is a software component that reliably and efficiently verifies the status of digital certificates from one or multiple CAs and provides services for the generation of time-stamps.

The main functions of the TOE are to:

- Receive and process OCSP requests on the status of the digital certificates from external users or applications (requesters), protecting the integrity of the requests and responses when managed by the TOE.
- Generate OCSP responses including the date and status of the certificates.
- Guarantee the non-repudiation, integrity and authentication of the responses, by means of the digital signature of these responses.
- Generate the OCSP´s key pairs in an HSM and manage the certificates issued by the OCSP Certification Authority (CA).
- Store information on the status of the certificates generated by one or more Certification Authorities. The status of a digital certificate is updated by downloading the revocation lists or the information provided by Certification Authorities (CA).
- Generate event logs so operators can monitor the system status, its security and to what extent the corporate specifications are being met.

- It is able to receive via the Internet and process time-stamping requests from external users or applications (requesters) to add timestamps, protecting the integrity of the requests when managed by the TOE.
- Generate timestamp responses that include the time of the request and the information that securely binds the stamp to the data.
- The integrity of the time-stamps produced by the TOE is protected when created and managed by the TOE and during transfer from the TOE to an external entity.
- Generate the time-stamping units' key pairs in an HSM and managing the certificates issued by the timestamp Certification Authority (CA).
- Connect with external trusted time sources to detect time drifts or jumps out of synchronization with UTC.
- Any external entity can verify the authentication of the time-stamps produced by the TOE.
- The TOE services (user identity and role management, TSU initialization, start of TSU operation, stop of TSU operation, finalization of TSU operation, generation of key pair, public key export for certificate request, certificate import, timestamp token generation and internal audit) are only used in an authorized way.
- Send the auditing logs generated to a SIEM.

The TOE provides the following additional functions to protect the TOE services:

- User authentication and access control.
- Auditing of security-relevant events produced within the TOE boundaries.

1.2.2 Required non-TOE hardware/software/firmware

The TOE relies upon the following IT additional hardware, software and firmware:

- A virtualization platform to run virtual macines (VM)
  The TOE supports the following virtualization platforms: VMWare vSphere, Nutanix, Microsoft Hyper-V, AWS and Azure.
- A server (Virtual Machine) running the operating system that is part of the PKI Hub system. Operating System time synchronized with an external source NTP required.
- An external reference Clock. The external reference Clock that is synchronized with UTC time such that
  - The time values the TSU uses in the time-stamp token shall be traceable to at least one of the real time values distributed by a UTC(k) laboratory.

    - The time included in the time-stamp token shall be synchronized with UTC within the accuracy defined in the policy and, if present, within the accuracy defined in the time-stamp token itself.
- A Cryptographic module, able to create digital signatures of the OCSP responses and time-stamp tokens, and is part of the PKI Hub System. This Cryptographic Module shall be a hardware based and that shall meet demonstrated conformance to FIPS PUB 140-2 level 3, FIPS 140-3 level 3, or EAL4 or higher in accordance to ISO/IEC 15408.
- When using the Certification Authorities information to check the status of the certificates, the Entrust CA Gateway and the Entrust Certificate Authority.
- When using CRLs to get certificate information, an HTTP or LDAP server hosting the CRLs in DER format.
- A Database Management System (DBMS) to host the certificate information. The TOE supports the following DBMSs: PostgreSQL, Oracle and SQL Server.
- A Security Information and Event Management (SIEM) to send the auditing logs. The TOE supports the following SIEMs: Splunk Enterprise and Splunk Cloud.

1.3 TOE Description

1.3.1 Physical scope of the TOE

The TOE is a software composed of several components that are downloaded from the vendor's portal at https://trustedcare.entrust.com. This secure portal requires authentication credentials to access the resources.

To download the TOE, log in to https://trustedcare.entrust.com, navigate to *PRODUCTS > Cryptographic Security Platform (CSP) > version 1.2*, and under *SOFTWARE DOWNLOADS* download the image file for installing the TOE on the platform of your choice.

- PKI Hub 1.3.0 for VMware vSphere, Hyper-V and Nutanix.
- PKI Hub 1.3.0 for Azure.
- PKI Hub 1.3.0 for Amazon Web Services

Download also the database scripts. To validate each downloaded file:

Generate the digest value. On a Windows machine, run the following command to generate the SHA256 digest of the <file> file: certutil -hashfile <file> < SHA256>.

On the *SOFTWARE DOWNLOADS* tab of the portal, click the *SHA-256* link displayed in the *Digest* column for the file.

Verify the displayed digest matches the generated one.

The TOE includes the guidance documentation which contains information on how to manage the TOE security functions. The guidance documentation is delivered to customers via a download from the vendor's Web site.

1.3.2 Logical scope of the TOE

The TOE Entrust Cryptographic Security Platform (CSP) | PKI Hub (hereafter, PKI Hub) is a software component running on an operating system that provides OCSP and time-stamps generation services to its requesters. Hardware and other software components that might be needed by the TOE to provide its services are considered part of the TOE operational environment. The TOE shall use a Hardware Secure Module (HSM) for the implementation of the cryptographic operations.

The below figure illustrates the general architecture of the OCSP service and how it interrelates with the network components (under the IETF RFC 6960 OCSP protocol). Entrust PKI Hub operates with external HSMs and requires connecting with one or more external NTP (Network Time Protocol) servers. External Certification Authorities provide OCSP certificates operated by Entrust PKI Hub.

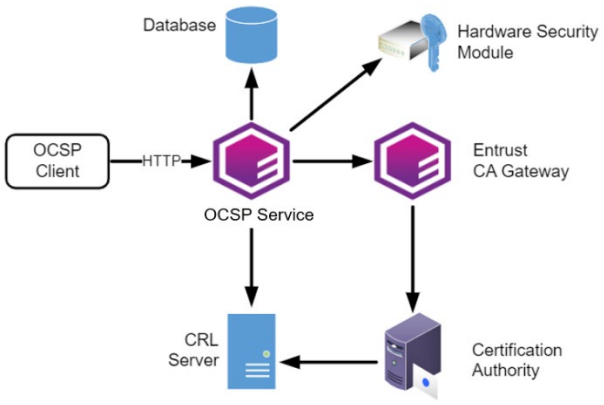

Figure 1: OCSP service Overview

To respond to OCSP requests, Entrust PKI Hub connects with different components. In this architecture:

- Multiple clients (users/applications) send requests to the validation service of Entrust PKI Hub.

- An OCSP request manager that handles the exchanges with the requesters, handling OCSP requests and providing corresponding OCSP responses.
- A Hardware Security Module (HSM) manages the OCSP signing key.
- A Database Management System (DBMS) hosts the certificate information.
- An external Certification Authority (CA) issues a PKI certificate from a Certificate Signing Request (CSR) of the OCSP service of the Entrust PKI Hub unit.
- An internal CertStatus feeder service API that offers an HTTP API to store information in the DBMS about the certificate issued and revoked by external CAs.
- When the TOE uses CRLs to get certification information, the CRL Server (HTTP/LDAP) provides certificate status information.
- A CRL Shim TOE; It's a background task in charge of periodically polling the CRL Server (HTTP/LDAP) to retrieve an updated CRL (and optionally a Serial Number list) and convert them into calls to the Cert Status Feeder.
- When the TOE uses CAs to get certification information, the Entrust CA Gateway provides certificate status information.
- A CA Gateway Shim. It's a background task in charge of periodically polling an Entrust CA Gateway to ask for certificate events (cert issuance and cert status changes) and convert them into calls to the Cert Status Feeder.

An OCSP service is the composition of

- An OCSP context, directly managed by the TOE;
- A key pair, stored within the HSM, outside of the TOE.

The below figure illustrates the general architecture of the time-stamps generation service and how it interrelates with the network components (under the IETF RFC 3161 timestamp protocol). Entrust PKI Hub operates with external HSMs and requires connecting with one or more external NTP (Network Time Protocol) servers. External Certification Authorities provide TSU certificates operated by Entrust PKI Hub.

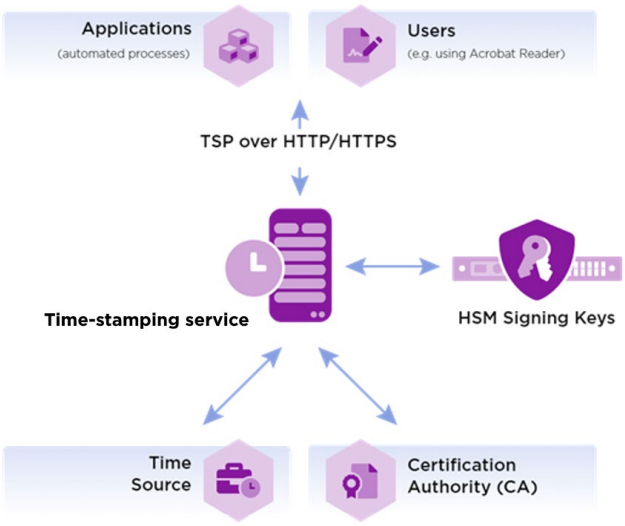

Figure 2: Time-stamp service Overview

To respond to timestamp requests, Entrust PKI Hub connects with different components. In this architecture:

- Multiple clients (users/applications) send requests to the time-stamping service of Entrust PKI Hub.
- One or several Hardware Security Modules (HSMs) manage the timestamp signing key.
- One or several Network Time Protocol (NTP) servers provide an accurate and reliable time source.
- An external Certification Authority (CA) issues a PKI certificate from a Certificate Signing Request (CSR) of the Time Stamping System of the Entrust PKI Hub unit.

The Time Stamping System is part of the operational environment where the TOE resides. It contains non-TOE elements such as the Cryptographic Module. The next Figure shows the details of the TOE in terms of functional components that are part of it, as well as the messages/operations exchanged with entities that belong to the operational environment, and others that do not (i.e. the CA, the external trusted time source).

The time-stamp service is composed of three modules (see figure 2):

- A time stamp request manager that handles the exchanges with the requesters, handling Time stamp request and providing corresponding time-stamps.
- A clock manager, in charge of the accurate synchronization with the external Trusted Time Source and the detections of incidents related to the time synchronization.

- A context manager, interacting with the crypto-module and the CA, in charge of the life-cycle of the key pair management. In particular:
  - Requesting the key pair generation within the crypto module;
  - Exporting the public key for the certificate request to the CA;
  - Importing the certificate generated by the CA;
  - Requesting the Crypto module signature of the generated Time-stamps.

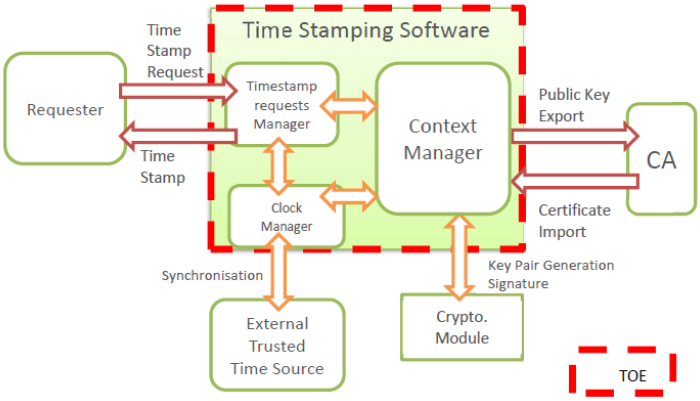

Figure 3: Overview of the TOE functional perimeter.

As depicted in the next Figure, the time-stamping software (the TOE) may operate several Time-stamping Units (TSU).

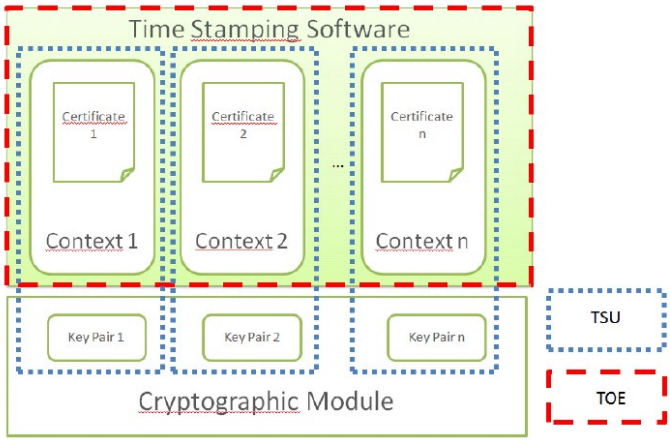

Figure 4; Time-stamping Unit.

A Time-stamping Unit is the composition of

- A time stamping context, directly managed by the TOE;
- A key pair, stored within the HSM, outside of the TOE.

The TOE shall handle the following user data:

- OCSP request: OCSP request sent by the requester to the TOE in order to obtain certificate status information.
- OCSP response: OCSP response generated and signed by the TOE based on the request information, and using the active private key of the OCSP context of the OCSP service.
- OCSP context: Set of data that comprises all the information needed to operate a OCSP service.
- Time-stamping request: Time-stamping request sent by the requester to the TOE in order to obtain a timestamp.
- Time-stamp: Time-stamp generated and signed by the TOE based on the time-stamp request information, and using the active private key of the time stamping context of the TSU.
- Time-stamp context: Set of data that comprises all the information needed to operate a TSU.
- Internal clock: Internal time used by the TSU that provides the date and time corresponding to UTC time included in each time-stamp.
- OCSP cryptographic key pair: Public key used by external entities to verify the integrity and origin authentication of the TOE signed OCSP responses, and handler to the private key used by the OCSP service to digitally sign the responses.
- Times-stamping cryptographic key pair: Public key used by external entities to verify the integrity and origin authentication of the TOE signed time-stamps, and handler to the private key used by the TSU to digitally sign the timestamps.
- Audit data: Audit records produced by the TOE.

The TOE supports the following user categories (roles):

- Requester of the TOE services: external entity that
  - sends time-stamping requests to the TOE and expects to receive a time-stamp signed by the TOE and
  - sends OCSP requests to the TOE and expects to receive a OCSP response signed by the TOE
- Security Officer: Responsible for operating the TOE and the trustworthy systems of the operational environment on a day-to-day basis. Authorized to install, configure, and maintain the TOE and the trustworthy systems of the operational environment for OCSP and time-stamping services management. Overall responsibility for administering the implementation of the security practices as well as administering the OCSP and time-stamping services.
- System Auditor: Authorized to view archives and audit logs of the TOE and the trustworthy systems of the operational environment.

Any user accessing the OCSP or the time-stamp generation service is regarded as a Requester. Those services are not authenticated and there is no access control mechanism. The TOE will not process the authentication data, and thus the requests will be treated as non-authenticated.

Authentication for all user categories shall be identity-based, except for the Requester, who accesses non-authenticated services.

The TOE, the OCSP and the Time-stamping system, including the crypto-module, are intended to be operated by a Validation Authority/Time Stamping Authority. The Security Officer and the System Auditor are located within the perimeter of the Validation/Time Stamping Authority and are considered as Trusted Roles. The requester is not part of the Validation/Time Stamping Authority but is in relation with the Validation/Time Stamping Authority as a consumer of the OCSP/Time-stamping services.

Other entities might be related to the TOE, though not directly connected through logical interfaces, such as a Certification Authority (CA).

2 Conformance Claims

The present Security Target conforms to the following assurance and functional requirements:

- General model of the "Part 1: Introduction and general model" of the Common Criteria Standard. November 2022. Version 2022. Revision 1.
- Functional Requirements of the "Part 2: Security functional components" of the Common Criteria Standard. November 2022, Version 2022, Revision 1.
- Functional Requirements of the "Part 2: Security functional components" extended of the Common Criteria Standard. November 2022, Version 2022, Revision 1.
- Assurance Requirements of the "Part 3: Security assurance components". November 2022, Version 2022, Revision 1, for the **EAL4 Common Criteria certification level, augmented with ALC_FLR.2**.

This Security Target does not claim conformance with any Protection Profiles.

3 Security Problem Definition

This section includes the assets, threats, organizational security policies and assumptions, that are part of the security problem definition. A relation between threats and assets is also included.

This information provides the basis for the Security Objectives specified in chapter Security Objectives, and for the Security Requirements for the TOE specified in chapter Security Requirements.

3.1 Assets

The TOE implements services that include user management, OCSP service configuration, start of OCSP service operation, stop of OCSP service operation, OCSP key destruction, generation of OCSP key pair, OCSP public key export for certificate request, OCSP certificate import, OCSP generation, time-stamping configuration, start of time-stamping operation, stop of time-stamping operation if the clock is detected as being out of the stated accuracy, time-stamp key destruction, time-stamp generation of key pair, time-stamp public key export for certificate request, time-stamp certificate import, timestamp token generation and internal audit.

The primary assets that need to be protected by the TOE are the following TOE internal data:

R.OCSP_REQUEST. This asset is the OCSP request sent by the requester to the TOE in order to obtain an OCSP response. This request shall contain the target certificate identifier.

R.OCSP_REQUEST shall be protected in integrity when inside the TOE.

R.OCSP_RESPONSE. The OCSP response is a signed electronic message including the certificate status information. Other information may be included. The OCSP response is generated based on the OCSP request information and signed using the active private key of the Validation Authority context.

R.OCSP_RESPONSE shall be protected in integrity and its origin shall be authenticated.

R.OCSP_CONTEXT. The OCSP context comprises all the information needed to operate an OCSP service. This asset contains the following elements:

- The configuration of the database where certificate information will be stored;
- The configuration of the HSM where key pairs will be stored;
- The type of source providing the certificate information;

- The configuration of the certificate source (URL, timeouts, etc.);
- The identifier of the OCSP policy that will be used to generate OCSP responses;
- The identifier of the key pair to be used;
- The certificate of the OCSP service public key. This certificate is issued by a certification authority, and it is included when the context state is in operational mode. The public key value within the certificate shall be the same as the public key of the key pair identified in the context.

R.OCSP_CONTEXT shall be protected in integrity.

R.OCSP_KEY_PAIR_PUB. This asset is the public key of a key pair configured in the OCSP context. The public key can be used by the requester and third parties to verify the integrity and authorship of the signed OCSP responses.

R.OCSP_KEY_PAIR_PUB shall be protected in integrity prior to being certified.

R.OCSP_KEY_PAIR_PRIV. This asset is the handler of or reference to the private key of a key pair configured in the OCSP context.

The private key, stored in the cryptographic module, is used by the OCSP service to digitally sign the OCSP response.

R.OCSP_KEY_PAIR_PRIV shall be protected in integrity and confidentiality.

Note: The private key itself shall be protected in integrity and in confidentiality by the cryptographic module.

R.TST_REQUEST. This asset is the time-stamping request sent by the requester to the TOE in order to obtain a time-stamp. This request shall contain:

- the hash of the document to be processed,
- identification of the hash algorithm used to calculate the hash of the document,
- other information may be included in R.TST_REQUEST.

It is important to notice that the request contains the hash of the document obtained with the hash algorithm defined in the request and not the document itself.

R.TST_REQUEST shall be protected in integrity when inside the TOE.

R.TST_TOKEN. The time-stamp token is a signed electronic message associating a document hash with a UTC time and a unique reference to the time-stamping policy. Other information may be included. The time-stamp is generated based on the time-stamp request information and signed using the active private key of the time stamping context of the TSU.

R.TST_TOKEN shall be protected in integrity.

R.TST_CONTEXT. The time-stamp context comprises all the information needed to operate a TSU. This asset contains the following elements:

- The identification of the time source to be used when the TOE manages multiple time source references;
- The accuracy of the time in the time-stamp tokens with respect to UTC.
- The configuration of the supported time-stamping policies. For each supported policy, the timestamp context contains:
    - The identifier of the time-stamping policy;
    - The identifier(s) of the supported hash algorithm(s);
- The identification of the default time-stamping policy;
- The identifier(s) of the key pair(s) to be used;
- The certificate of the TSU public key. This certificate is issued by a certification authority, and it is included when the context state is in operational mode. The public key value within the certificate shall be the same as the public key of the key pair identified in the context.

R.TST_CONTEXT shall be protected in integrity.

R.DATE_AND_TIME. This asset provides the date and time (reference time) to be included in each timestamp token. Associated with this date and time is:

- A synchronization state (internal clock manager), that indicates whether the clock is synchronized with UTC or not.
- A synchronization precision value.

R.DATE_AND_TIME shall be protected in integrity.

R.TST_KEY_PAIR_PUB. This asset is the public key of a time-stamping context. The public key can be used by the requester and third parties to verify the integrity and authorship of the signed time-stamp.

R.TST_KEY_PAIR_PUB shall be protected in integrity prior to being certified.

R.TST_KEY_PAIR_PRIV. This asset is the handler of or reference to the private key of a time-stamping context.

The private key, stored in the cryptographic module, is used by the TSU to digitally sign the time-stamps.

R.TST_KEY_PAIR_PRIV shall be protected in integrity and confidentiality.

Note: The private key itself shall be protected in integrity and in confidentiality by the cryptographic module.

R.TLS_CONTEXT. The TLS context comprises all the information needed to operate the client/server TLS connections. This asset contains the following elements:

- The private key to be used for the Auditor UI (Grafana) HTTPS (TLS) service.
- The certificate of the Auditor UI service public key. This certificate is issued by a certification authority, and it is included when the context state is in operational mode. The public key value within the certificate shall be the key pair of the private key of the context.
- The configuration of the SIEM to forward the audit logs (URL, timeout, etc.), including the certificate to validate the HTTPS (TLS) connection.

R.TSF_DATA: TSF data, including:

- Authentication data of TOE users (administrators and auditors), which shall be protected in confidentiality and integrity.
- Non-confidential user/role related data (identifier, access control lists, role definitions, etc.). This data shall be protected in integrity.

R.AUDIT_DATA. Internal audit records and that shall be protected in integrity.

Next table correlates the TOE internal data types explained above with those data types considered in the formalization of the security functional requirements (SFR):

TOE internal data type	SFR-related data type
R.OCSP_REQUEST	User data (1)
R.OCSP_RESPONSE	
R.OCSP_CONTEXT	
R.OCSP_KEY_PAIR_PUB	
R.OCSP_KEY_PAIR_PRIV	
R.TST_REQUEST	
R.TST_TOKEN	
R.TST_CONTEXT	
R.DATE_AND_TIME	
R.TST_KEY_PAIR_PUB	
R.TST_KEY_PAIR_PRIV	
R.AUDIT_DATA	
R.TLS_CONTEXT	TSF data (2)

R.TSF_DATA	TSF data (2)

(1) data for the user that does not affect the operation of the TSF (TOE Security Functionality). For example, in the case of R.AUDIT_DATA, the audit records generated internally in the TOE are intended to be revised by the Auditor.
(2) data for the operation of the TOE upon which the enforcement of the SFR relies.

3.2 Threats

The expected attackers are qualified so as to have Enhanced-Basic attack potential, in accordance with the security assurance given by AVA_VAN.3 Focused vulnerability analysis.

The expected threat agents are:

TA.EXTERNAL

This agent represents an entity that does not hold any authorized role to operate or interact with the TOE.

This agent may operate through the remote or local interfaces of the TOE, or even have direct physical access to the TOE. Examples of this threat agent are: unauthorized TOE personnel, cybercriminals, and hackers in general.

TA.INSIDER

This agent represents an entity that holds an authorized role to operate or interact with the TOE, except for role Security Officer, and which has the intention to compromise the TOE assets. This agent may operate through the remote or local interfaces of the TOE, or even have direct physical access to the TOE. These threat agents are the Auditors and the Requester of the TOE services.

TA.INADVERTENT

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

The expected threats to the TOE may be:

T.CONTEXT_ALTERATION

A TA.INSIDER might change the operational OCSP or time-stamp contexts (R.OCSP_CONTEXT and R.TST_CONTEXT) with the purpose to or with the consequence of using a context with weaker security attributes (e.g. weak hash algorithms), a compromised private key for which the certificate revocation has not been processed yet, etc.

T.DATE_AND_TIME_ALTERATION

A TA.INSIDER might change the reference date and time and/or the synchronization state of R.DATE_AND_TIME with the purpose to make the TOE issue signed time-stamps with an intended time that deviates from the actual UTC date and time. The threat can be materialized in two ways:

(1) The TA.INSIDER sets the time of the internal clock with an arbitrary date in the past or in the future that is outside the range of clock accuracy.

(2) The TA.INSIDER sets the time of the internal clock with an arbitrary date in the past or in the future that is inside the range of clock accuracy, and performs this attack over again until a gap greater than the range of the clock accuracy is reached.

T.PRIVATE_KEY_ALTERATION

A TA.EXTERNAL or a TA.INSIDER might modify or alter the R.OCSP_KEY_PAIR_PRIV or R.TST_KEY_PAIR_PRIV while being operated inside the PKI Hub, resulting in a loss of integrity and/or availability of the R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV.

For instance, a TA.INSIDER such a malicious auditor without authorization to change the R.OCSP_KEY_PAIR_PRIV reference to another private key that may not be stored in a HSM or that may produce non verifiable OCSP responses.

T.PUBLIC_KEY_ALTERATION

A TA.EXTERNAL or a TA.INSIDER might modify or alter the R.OCSP_KEY_PAIR_PUB or R.TST_KEY_PAIR_PUB before creating the certificate request for further export, resulting in a loss of integrity of the R.OCSP_KEY_PAIR_PUB/ R.TST_KEY_PAIR_PUB.

T.PRIVATE_KEY_DERIVATION

A TA.EXTERNAL or a TA.INSIDER might derive all or parts of private key referred by R.OCSP_KEY_PAIR_PRIV or R.TST_KEY_PAIR_PRIV using knowledge gained about, for example, the corresponding public key, the cryptosystem and the key generation process. This knowledge might enable the attacker to conduct certain cryptanalysis attacks that does not require access to the environment where the private key is stored.

Notice that the private keys referred R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV are intended to be stored in the HSM outside the perimeter of the TOE. Therefore, this threat apply mainly on the private key referred by R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV and not on R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV themselves. However, this threat applies in the case where R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV refers to a private key generated with a weak algorithm.

T.PRIVATE_KEY_DISCLOSURE

A TA.EXTERNAL or a TA.INSIDER might disclose all or part of private key referred by R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV over logical TOE interface or physical interface of the operational environment by using covert channel mechanisms.

Notice that the private keys referred by R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV are intended to be stored in the HSM outside the perimeter of the TOE. Therefore, this threat applies mainly on the private key referred by R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV and not on R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV themselves. However, this threat applies in the case where R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV refers to a private key generated with a weak algorithm.

T.CRYPTO

A TA.EXTERNAL or a TA.INSIDER might deduce the R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV from the respective R.OCSP_KEY_PAIR_PUB/R.TST_KEY_PAIR_ PUB or create a forged digital signature due to the use of a weak cryptographic suite by TOE for either key pair generation or digital signature operation.

T.MISUSE

A TA.EXTERNAL or a TA.INSIDER, who has access to the TOE services, uses these services without proper authorizations or in a manner for which they are not intended, having an impact on the R.OCSP_REQUEST, R.OCSP_RESPONSE, R.OCSP_CONTEXT, R.OCSP_KEY_PAIR_PUB, R.OCSP_KEY_PAIR_PRIV, R.TST_REQUEST, R.TST_TOKEN, R.TST_CONTEXT, R.DATE_AND_TIME, R.TST_KEY_PAIR_PUB, R.TST_KEY_PAIR_PRIV, R.AUDIT_DATA or R.TSF_DATA.

For instance, a TA.INSIDER such a malicious auditor without authorization to generate key pairs (R.OCSP_KEY_PAIR_PUB/R.TST_KEY_PAIR_PUB and R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV) may misuse the TOE services to do so.

T.INSECURE_INITIALISATION

A TA.EXTERNAL or a TA.INSIDER might initialize the TOE with insecure R.TSF_DATA.

T.AUDIT_ALTERATION

A TA.EXTERNAL or TA.INSIDER might alter the TOE R.AUDIT_DATA.

T.UNRELIABLE_OCSP_RESPONSE

The requester of TOE Services receives an unreliable OCSP response.

T.UNRELIABLE_TST

The requester of TOE Services receives an unreliable TST.

3.2.1 Relation between threats and assets

Asset	Security dimension(s)	Threat(s)
R.OCSP_REQUEST	Integrity	T.MISUSE
R.OCSP_RESPONSE	Integrity	T.MISUSE T.UNRELIABLE_OCSP_RESPONSE
	Origin authentication	T.MISUSE T.UNRELIABLE_OCSP_RESPONSE
R.OCSP_CONTEXT	Integrity	T.CONTEXT_ALTERATION T.MISUSE
R.OCSP_KEY_PAIR_PUB	Integrity	T.PUBLIC_KEY_ALTERATION T.MISUSE
R.OCSP_KEY_PAIR_PRIV	Confidentiality	T.PRIVATE_KEY_DERIVATION T.PRIVATE_KEY_DISCLOSURE T.MISUSE T.CRYPTO
	Integrity	T.PRIVATE_KEY_ALTERATION T.MISUSE
R.TST_REQUEST	Integrity	T.MISUSE
R.TST_TOKEN	Integrity	T.MISUSE T.UNRELIABLE_TST
	Origin authentication	T.MISUSE T.UNRELIABLE_TST

R.TST_CONTEXT	Integrity	T.CONTEXT_ALTERATION T.MISUSE
R.DATE_AND_TIME	Integrity	T.DATE_AND_TIME_ALTERATION T.MISUSE
R.TST_KEY_PAIR_PUB	Integrity	T.PUBLIC_KEY_ALTERATION T.MISUSE
R.TST_KEY_PAIR_PRIV	Confidentiality	T.PRIVATE_KEY_DERIVATION T.PRIVATE_KEY_DISCLOSURE T.MISUSE T.CRYPTO
	Integrity	T.PRIVATE_KEY_ALTERATION T.MISUSE
R.TLS_CONTEXT	Integrity	T.CONTEXT_ALTERATION T.MISUSE
R.TSF_DATA (Authentication data)	Confidentiality	T.MISUSE
	Integrity	T.MISUSE
R.TSF_DATA (non-confidential data)	Integrity	T.MISUSE T.INSECURE_INITIALISATION
R.AUDIT_DATA	Integrity	T.MISUSE T.AUDIT_ALTERATION

Table 1. Relationship between threats and assets

3.3 Organizational security policies

OSP.ALGORITHMS

Only approved algorithms and algorithm parameters defined as acceptable for being used in R.OCSP_KEY_PAIR_PUB/R.OCSP_KEY_PAIR_PRIV and R.TST_KEY_PAIR_PUB/R.TST_KEY_PAIR_PRIV pair generation and OCSP responses and timestamp token signing shall be used by the TOE.

This includes the generation of random numbers and the quality of the R.OCSP_KEY_PAIR_PUB/R.OCSP_KEY_PAIR_PRIV and R.TST_KEY_PAIR_PUB/R.TST_KEY_PAIR_PRIV pairs generated.

Approved algorithms and algorithm parameters defined as acceptable shall be used to ensure the confidentiality and integrity of private key referred by

R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV, and the integrity of R.OCSP_KEY_PAIR_PUB/R.TST_KEY_PAIR_PUB.

The TOE shall support cryptographic algorithms and key lengths conformant to the rules defined by ETSI TS 119 312 [ETSI 119 312] and [SOG-IS-Crypto].

OSP.OCSP_SERVICE

The TOE shall generate OCSP responses in conformity with the OCSP service policy. Responses shall be signed using the private key referenced in the R.OCSP_CONTEXT.

OSP.TIMESTAMP_SERVICE

The TOE shall generate timestamps in conformity with the time-stamping policy. Time-stamps shall be signed using the private key referenced in the R.TST_CONTEXT.

OSP.OCSP_REQUEST_MGMT

The OCSP protocol implemented by the TOE shall ensure that the OCSP response R.OCSP_RESPONSE is generated in conformity with the data received in the request R.OCSP_REQUEST.

OSP.TIMESTAMP_REQUEST_MGMT

The time-stamping protocol implemented by the TOE shall ensure that the time-stamp R.TST_TOKEN is generated in conformity with the data received in the request R.TST_REQUEST.

OSP.CLOCK

During the initialization of the TSU, the reference time of the R.DATE_AND_TIME shall be checked to ascertain that it is synchronized with a trusted external UTC time source.

3.4 Assumptions

A.VAS

The PKI Hub System meets the requirements related to the laid down in [EN319411-2] or equivalent. In addition, the communication network where the TOE operates is secured to prevent intrusions and other forms of cyberattacks.

The operational environment also implements a secure communication channel, such as HTTPs or similar, to protect the confidentiality and integrity of the information exchanged between the TOE and external entities.

A.ACCESS_PROTECTED

The TOE is protected by physical and organizational protection measures implemented by the TOE environment. Those measures shall restrict the TOE physical access (e.g. for administration purposes) to authorized persons only and shall require dual control. These measures counteract threats that might try to physically manipulate the TOE operational environment with the intent to:

- derive all or part of the private key referred by R.OCSP_KEY_PAIR_PRIV/ R.TST_KEY_PAIR_PRIV (by side channel for example), and/or o alter received R.OCSP_REQUEST/R.TST_RQUEST, generated R.OCSP_RESPONSE/R.TST_RESPONSE, R.OCSP_CONTEXT/ R.TST_CONTEXT, R.OCSP_KEY_PAIR_PUB/R.TST_KEY_PAIR_PUB, R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV, R.AUDIT_DATA or R.TSF_DATA, and/or
- make R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PRIV, R.TSF_DATA (VAD or RAD) or R.AUDIT_DATA unavailable, and/or
- destroy the TOE by deliberate action.

A.REF_TIME

It is assumed that no attack can simultaneously compromise the reference time and the TOE clock checking mechanism, e.g., by changing the synchronization state.

It is supposed that it will be processed, during the time-stamping unit initialization, to a verification of a correct initialization of the time reference.

Moreover it is supposed that no attack can compromise simultaneously and in a coherent way the values of a time-stamping unit internal clock and the time reference.

Application note

As mentioned in section 4.2.3, the TOE is intended to be operated by a Trusted Service Provider operating time-stamping authority. Therefore, the TOE is intended to be operated in a secured environment that meets the requirements of the [EN319421] and provide appropriate security measures to limit simultaneous attacks on the time reference and the TOE clock checking mechanism. On top of these requirements, we provide the following recommendations to meet the assumption.

The initialization of the time reference must include, if applicable, the verification of the wires between the time-stamping unit and the external sources. In the case of radio sources, this verification must also include the wires to the antennas.

The time reference can be obtained from several manners, for example with the assistance:

- of an authenticated single external source,
- of not authenticated multiple external sources,
- of an atomic clock located in the monitoring environment of the time-stamping system.

The risk of a simultaneous compromising and in a coherent way of the values of the time-stamping unit internal clock and of the time reference can for example be limited by:

- the choice of different technologies (in particular when an atomic clock provides the time reference, it should not also make function of internal clock),
- the selection of different locations.

A.OCSPRESPONSE_VERIFICATION

The requester verifies the correctness of the OCSP responses received from the TOE and ensures its preservation, if needed. For that, the requester:

- Verifies the digital signature of the response.
- Checks if the certificate identifier received in the OCSP response is the same as the one included in the corresponding request sent to the TOE.

A.TIMESTAMP_VERIFICATION

The requester verifies the correctness of the time-stamps received from the TOE and ensures its preservation, if needed. For that, the requester:

- Verifies the digital signature of the time-stamp.
- Checks if the hash within the received time-stamp is the same as the one included in the corresponding request sent to the TOE.

A.AUDIT_REVIEW

TOE Auditors check the audit trails on a regular basis, and notify the corresponding authority in the case that an incident occurred.

A.CA

The Certification Authority that issues the certificates to the TOE implements a set of practices in conformity with their CP/CPS.

A.CERTIFIED_CM

The cryptographic module used by the TOE to digitally sign the OCSP responses and the timestamp token is a certified device that meets:

- the requirements of [EN319411-2] related to the OCSP service or equivalent.
- or the following:
    - meets the requirements identified in ISO/IEC 19790, level 3 or higher;

      NOTE: Demonstrated conformance to FIPS PUB 140-2/-3, level 3 is considered as fulfilment of this requirement.

    - meets the requirements identified in [CEN TS 419 221-2] or [CEN TS 419 221-4] or [CEN TS 419 221-5]; or
    - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408, or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

A.SECURE_BACKUP

If the cryptographic module used by the TOE allows backup of OCSP and time-stamping private keys, they are copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see A.ACCESS_PROTECTED). The personnel authorized to carry out this function are limited to those requiring to do so under the established practices.

Any backup copies of the OCSP/TSU private signing keys are protected by the cryptographic module to ensure its integrity and confidentiality before being stored outside that device.

After expiration of the certificate associated to the private key, all backups of the key are destroyed or made unable to be used by appropriate means.

4 Security Objectives

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent to counter the identified threats, as well as comply with the identified organizational security policies and assumptions.

4.1 Security objectives for the TOE

O.AUDIT Generation and Export of Audit Data

The TOE shall audit the following events:

- TOE initialization.
- TOE start-up.
- Start of OCSP service operation.
- Stop of OCSP service operation.
- Generation of R.OCSP_KEY_PAIR_PUB/ R.OCSP_KEY_PAIR_PRIV pairs.
- Export of R.OCSP_KEY_PAIR_PUB for certificate request.
- Changes in the R.OCSP_CONTEXT, including changes in the OCSP policy, the identifier of the key pair to be used, and the certificate of the OCSP service public key.
- Destruction of R.OCSP_KEY_PAIR_PUB/ R.OCSP_KEY_PAIR_PRIV pairs.
- OCSP response generation.
- Start of TSU operation.
- Stop of TSU operation.
- Desynchronization of the TOE.
- Generation of R.TST_KEY_PAIR_PUB/ R.TST_KEY_PAIR_PRIV pairs.
- Export of R.TST_KEY_PAIR_PUB for certificate request.
- Changes in the R.TST_CONTEXT, including changes in the time source to use, supported time-stamping policies, identification of the default time-stamping policy, the identifier of the default time-stamping policy, the identifier(s) of the key pair(s) to be used, and the certificate of the TSU public key.
- Updates of the internal clock values, including the date, time and the synchronization state.
- Destruction of R.TST_KEY_PAIR_PUB/ R.TST_KEY_PAIR_PRIV pairs.
- Time-stamp generation.
- Unsuccessful authentication.
- Modification of TOE user management data.
- Adding new users or roles.
- Deleting users or roles.

The audit data shall associate each auditable event with the identity of the user that caused the event. For the OCSP response generation event, the audit data shall incorporate the identifier of the key pair used in the process. For the time-stamp generation event, the audit data shall incorporate the time-stamping policy and the identifier of the key pair used in the process. The integrity of the audit trail shall be ensured. The TOE shall export the audit data upon request of the Auditor. The TOE shall provide the management function for the audit to the Auditor only.

O.USER_AUTHENTICATION Authentication of TOE Users

The TOE shall be able to identify and authenticate the users acting with a defined role, before allowing any access to TOE protected assets (TOE services – except OCSP and time-stamp generation services, for which authentication is needed – and TOE internal data). Identification and authentication shall be based on user identity.

O.RBAC Role-based Access Control to TOE Services

The TOE shall restrict the access to its assets (TOE services – except OCSP and time-stamp generation service, for which no access control is needed – and TOE internal data) depending on the user role, allowing user access only to those services and data explicitly authorized to the assigned role. Assignment of services to roles shall be done either by explicit action of an Administrator or by default.

O.PUBLIC_KEY_MANAGEMENT Secure Management of Public Key

The TOE shall check the integrity of the R.OCSP_KEY_PAIR_PUB and R.TST_KEY_PAIR_PUB when it is under the control of the TOE and before it is exported for certification.

O.SYNCHRONISATION Stop of operation under asynchrony with UTC time source

The TOE shall stop issuing timestamps if the internal clock is out of the specified accuracy.

O.AUDIT_PROTECTION Protection of audit data

The TOE shall implement mechanisms to prevent a T.EXTERNAL and T.INSIDER from modifying R.AUDIT_DATA.

O.CRYPTO Secure Cryptographic Operations

Only approved algorithms and algorithm parameters defined as acceptable for being used in R.OCSP_KEY_PAIR_PUB/R.OCSP_KEY_PAIR_PRIV and R.TST_KEY_PAIR_PUB/R.TST_KEY_PAIR_PRIV pair generation and OCSP responses and time-stamps signing shall be used by the TOE.

The TOE shall support cryptographic algorithms and key lengths conformant to the rules defined by the relevant national CC Certification Body.

O.OCSP_R Secure OCSP Responses

The TOE shall issue OCSP responses with valid information. Specific information included in OCSP responses contributes to this response being considered with integrity, secure and so that its Verifier can fully trust the information received.

O.TST Secure Time Stamp Tokens

The TOE shall issue Time Stamp Tokens with valid information. Specific information included in Time Stamp Tokens contributes to this token being considered with integrity, secure and so that its Verifier can fully trust the information received.

4.2 Security objectives for the operational environment

The following security objectives relate to the TOE environment. This includes the rest of the OCSP Service System (Operating System, Drivers, HW and OCSP service) and Time Stamping System (Operating System, Drivers, HW and time-stamping service) as well as the procedures for the secure operation of the TOE.

OE.ORS OCSP Responses System

The OCSP Responses System shall meet the requirements related to the OCSP laid down in [EN319411-2] or equivalent. In addition, the communication network where the TOE operates shall be secured to prevent intrusions and other forms of cyber-attacks. The operational environment shall also implement a secure communication channel, such as HTTPs or similar, to protect the confidentiality and integrity of the information exchanged between the TOE and external entities.

OE.TSS Time Stamping System

The Time Stamping System shall meet the requirements laid down in [EN319421] or equivalent. In addition, the communication network where the TOE operates shall be secured to prevent intrusions and other forms of cyber-attacks. The operational environment shall also implement a secure communication channel, such as HTTPs or similar, to protect the confidentiality and integrity of the information exchanged between the TOE and external entities.

OE.KEY_PAIR_GENERATION Public Key/Private Key Pair Generation

For the R.OCSP_KEY_PAIR_PUB/R.OCSP_KEY_PAIR_PRIV and R.TST_KEY_PAIR_PUB/R.TST_KEY_PAIR_PRIV pair generation, the TOE

environment shall implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority.

Note: See ETSI TS 119 312 [ETSI 119 312] and [SOG-IS-Crypto] for guidance on signature algorithms and their parameters.

OE.PRIVATE_KEY_MANAGEMENT Secure Management of Private Key

The TOE environment shall ensure the confidentiality and integrity of the private key referred by R.OCSP_KEY_PAIR_PRIV and R.TST_KEY_PAIR_PRIV. This includes protection against disclosing completely or partly the private key referred by R.OCSP_KEY_PAIR_PRIV and R.TST_KEY_PAIR_PRIV in clear through any logical interface. For confidentiality and integrity purposes, the TOE environment shall also implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority.

OE.PROTECT_ACCESS Prevention of Unauthorized Physical Access

The TOE shall be protected by physical, logical and organizational protection measures implemented by the TOE environment in order to prevent any TOE modification, as well as any protected assets disclosure.

Those measures shall restrict the TOE usage and access to authorized persons only and shall require dual control. The TOE operational environment shall follow the policy requirements established in in [EN319411-2].

OE.PERSONNEL Liability and Training

The personnel that have access to the TOE or use its services shall be aware of civil, financial and legal responsibilities, as well as the obligations they have to face, depending on their role. The personnel shall be trained on correct usage of the TOE.

OE.SECURE_INIT Secure Initialization Procedures

Procedures and controls in the TOE environment shall be defined and applied to permit the secure set-up and initialization of the TOE services within a TSP system in compliance with the requirements of the EU directive and the Policy for certification authorities issuing qualified certificates [8]. This includes the initial configuration of R.TSF_DATA, as well as OCSP and TSU configuration and the start of OCSP/TSU operation by the security officer. During the initialization of the TSU, the security officer shall check that the reference time of the **R.DATE_AND_TIME** is synchronized with a trusted external UTC time source.

Moreover, the TOE environment shall guarantee that no attack can compromise simultaneously and in a coherent way the value of the reference time and the synchronization state. This can be achieved by, for example:

- Selecting different technologies (e.g. for the atomic clock, if used as the time reference in the TOE environment)
- Selecting different locations, if the time reference is calculated based on the values provided by more than one external source which the TOE is connected to.

OE.SECURE_OPER Secure Operating Procedures

Procedures and controls in the TOE environment shall be defined and applied to permit the secure operation of the TOE services within a TSP system in compliance with the requirements of the Regulation (EU) n.910/2014 and the Policy for certification authorities issuing qualified certificates [8].

OE.OCSPRESPONSE_VERIFICATION OCSP Response verification

The requester verifies the correctness of the OCSP responses received from the TOE and ensures its preservation, if needed. For that, the requester:

- Verifies the digital signature of the response.
- Checks if the certificate identifier received in the OCSP response is the same as the one included in the corresponding request sent to the TOE.

OE.TIMESTAMP_VERIFICATION Time-stamp verification

The requester shall verify the correctness of the time-stamps received from the TOE and ensure its preservation, if needed. For that, the requester shall:

- Verify the digital signature of the time-stamp.
- Check if the hash within the received time-stamp is the same as the one included in the corresponding request sent to the TOE.

OE.AUDIT_REVIEW Audit review

TOE Auditors shall check the audit trails on a regular basis, and notify the corresponding authority in the case that an incident occurred.

OE.CA Certification Authority

The Certification Authority that issues the certificates to the TOE shall implement a set of practices in conformity with their CP/CPS.

Note: See ETSI EN 319 411-2 [ETSI 319 411-2] Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.

OE.CERTIFIED_CM Certified cryptographic module

The cryptographic module used by the TOE to digitally sign the OCSP responses shall be a certified hardware device with demonstrated conformance to FIPS PUB

140-2 level 3, FIPS 140-3 level 3, or EAL4 or higher in accordance to ISO/IEC 15408.

OE.SECURE_BACKUP Secure backup of private keys

If the cryptographic module used by the TOE allows backup of OCSP and time-stamping private keys and the associated sensitive information, they shall be copied, stored and recovered only by personnel in trusted roles (see OE.PERSONNEL) using, at least, dual control in a physically secured environment (see OE.PROTECT_ACCESS). The personnel authorized to carry out this function shall be limited to those required to do so under the established practices.

Any backup copies of the OCSP/time-stamping private signing keys shall be protected by the cryptographic module to ensure its integrity and confidentiality before being stored outside that device. After expiration of the certificate associated to the private key, all backups of the key shall be destroyed or made unable to be used by appropriate means.

4.3 Security objectives rationale

The following table shows the correspondence between the security objectives applicable to the TOE and the environment and the countered threats, the assumptions and the organizational security policies.

	T.CONTEXT_ALTERATION	T.PRIVATE_KEY_ALTERATION	T.PUBLIC_KEY_ALTERATION	.PRIVATE_KEY_DERIVATION	T.PRIVATE_KEY_DISCLOSURE	T.CRYPTO	T.MISUSE	T.INSECURE_INITIALISATION	T.AUDIT_ALTERATION	T.UNRELIABLE_OCSP_RESPONSE	T.DATE_AND_TIME_ALTERATION	T.UNRELIABLE_TST
O.AUDIT	X	X	X				X	X			X	
O.USER_AUTHENTICATION		X	X				X					
O.RBAC		X	X				X					

O.CRYPTO				X		X						
O.PUBLIC_KEY_MANAGEMENT			X									
O.AUDIT_PROTECTION									X			
O.OCSP_R										X		
O.SYNCHRONISATION											X	
O.TST												X
OE.ORS							X					
OE.KEY_PAIR_GENERATION				X								
OE.PRIVATE_KEY_ MANAGEMENT		X			X							
OE.PROTECT_ACCESS					X							
OE.PERSONNEL	X	X	X		X		X	X			X	
OE.SECURE_INIT								X				
OE.SECURE_OPER					X		X					
OE.OCSPRESPONSE_VERIFICATION												
OE.AUDIT_REVIEW	X	X	X				X	X			X	
OE.CA												
OE.CERTIFIED_CM					X							
OE.SECURE_BACKUP		X			X							
OE.TSS												
OE.TIMESTAMP_VERIFICATION												

Table 2. Security Objectives Rationale I

	OSP-ALGORITHMS	OSP.OCSP_SERVICE	OSP.OCSP_REQUEST_MGMT	OSP_TIMESTAMP_REQUEST_MGMT	OSP_CLOCK	A.VAS	A.ACCESS_PROTECTED.	A.OCSPESPONSE_VERIFICATION	A.AUDIT_REVIEW	A.CA	A.CERTIFIED_CM	A.SECURE_BACKUP	A.REF_TIME	A.TIMESTAMP_VERIFICATION
O.AUDIT		X												
O.USER_AUTHENTICATION														
O.RBAC														
O.CRYPTO	X													
O.PUBLIC_KEY_MANAGEMENT	X													
O.AUDIT_PROTECTION														
O.OCSP_R														
OE.ORS						X								
OE.KEY_PAIR_GENERATION	X													
OE.PRIVATE_KEY_ MANAGEMENT	X													
OE.PROTECT_ACCESS							X							
OE.PERSONNEL														
OE.SECURE_INIT					X								X	
OE.SECURE_OPER														
OE.OCSPRESPONSE_VERIFICATION			X					X						

OE.AUDIT_REVIEW		X							X					
OE.CA										X				
OE.CERTIFIED_CM											X			
OE.SECURE_BACKUP												X		
OE.TSS														
OE.TIMESTAMP_VERIFICATION				X										X

Table 31. Security Objectives Rationale II

Security objectives coverage is met as each threat, assumption and organizational security policy is addressed by at least one security objective, and every security objective is mapped with at least one threat, assumption or organizational security policy.

Next, the rationale for each matching is provided:

T.CONTEXT_ALTERATION is a threat by which a TA.INSIDER changes the operational OCSP context (R.OCSP_CONTEXT) with the purpose to or with the consequence of using a context with weaker security attributes (e.g. weak hash algorithms), a compromised private key for which the certificate revocation has not been processed yet, etc. This threat is countered by **O.AUDIT** (Generation and Export of Audit Data), which establishes the need to record events relevant to changes in the context, and **OE.AUDIT_REVIEW** (Audit review), which ensures that the auditors regularly check the audit trails and notify in the case that an incident occurs. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training), which covers the awareness and training of the personnel that use the TOE. This objective diminishes the threat in both cases (TA.INSIDER or TA.INADVERTENT) due to the liability issues, and also in the case of a TA.INADVERTENT because of the training undertaken.

T.PRIVATE_KEY_ALTERATION is a threat where a TA.EXTERNAL or a TA.INSIDER modifies or alters the private key while being operated inside the OCSP service, resulting in a loss of integrity and/or availability of the private key. This threat is countered by several security objectives. First, audit trails related to changes in the private key (Generation of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs, Destruction of R.KEY_PAIR_PUB/ R.KEY_PAIR_PRIV pairs) are recorded by the TOE (**O.AUDIT** (Generation and Export of Audit Data)) and later on reviewed by the auditors (**OE.AUDIT_REVIEW** (Audit review)). This ensures that if any adverse action towards changing the private key occurs, in particular those that trigger either of these two events, then the necessary information is recorded to trace back to the corresponding user and date. This is relevant for TA.INSIDER threat

agent, who shall be authenticated in the TOE. For threat agents TA.EXTERNAL, this threat is countered by authentication and access control mechanisms implemented by the TOE, and represented by the objectives **O.USER_AUTHENTICATION** (Authentication of TOE Users) and **O.RBAC** (Role-based Access Control to TOE Services) respectively. This threat is also countered by **OE.PRIVATE_KEY_MANAGEMENT** (Secure Management of Private Key), by which the TOE environment has to ensure the confidentiality and integrity of the private key. Also, for confidentiality and integrity purposes, the TOE environment has to implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority. This threat is also diminished by **OE.PERSONNEL** (Liability and Training) due to the liability issues involved. Finally, the impact derived from this threat is mitigated by a secure backup of OCSP private keys during which the cryptographic module preserves the integrity and confidentiality of the keys, if the cryptographic module used by the TOE permits the backup operation (**OE.SECURE_BACKUP** (Secure backup of private keys)). By having a backup of the private keys, the TOE is able to restore it to a previous (valid) value if the alteration is detected.

T.PUBLIC_KEY_ALTERATION is a threat where a TA.EXTERNAL or a TA.INSIDER modifies or alters the public key before creating the certificate request for further export, resulting in a loss of integrity of the public key. This threat is countered by several security objectives. First, audit trails related to changes in the public key (Generation of R.KEY_PAIR_PUB/ R. KEY_PAIR_PRIV pairs, Destruction of R.KEY_PAIR_PUB/ R.KEY_PAIR_PRIV pairs) and export of the public key (Export of R.KEY_PAIR_PUB for certificate request) are recorded by the TOE (**O.AUDIT** (Generation and Export of Audit Data)) and later on reviewed by the auditors (**OE.AUDIT_REVIEW** (Audit review)). This ensures that if any adverse action towards changing the public key occurs, in particular those that trigger either of these two events, then the necessary information is recorded to trace back to the corresponding user and date. This is relevant for TA.INSIDER threat agent, who shall be authenticated in the TOE. For threat agents TA.EXTERNAL, this threat is countered by authentication and access control mechanisms implemented by the TOE, and represented by the objectives **O.USER_AUTHENTICATION** (Authentication of TOE Users) and **O.RBAC** (Role-based Access Control to TOE Services) respectively. This threat is also countered by **O.PUBLIC_KEY_MANAGEMENT** (Secure Management of Public Key), by which the TOE ensures the integrity of the public key when it is under the control of the TOE and before it is exported for certification. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training) due to the liability issues involved.

T.PRIVATE_KEY_DERIVATION is a threat by which a TA.EXTERNAL or a TA.INSIDER derives all or parts of the private key using knowledge gained about,

for example, the corresponding public key, the cryptosystem and the key generation process. This knowledge might enable the attacker to conduct certain cryptanalysis attacks that does not require access to the environment where the private key is stored. This threat is countered by two security objectives. First, **OE.KEY_PAIR_GENERATION** (Public Key/Private Key Pair Generation) states that the TOE environment has to implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority to be used for the key pair generation. Second, this threat is counteracted by **O.CRYPTO** (Secure Cryptographic Operations), by which only strong approved algorithms and algorithm parameters defined as acceptable for being used in R.KEY_PAIR_PUB/R.KEY_PAIR_PRIV pair generation and OCSP signing shall be used by the TOE.

T.PRIVATE_KEY_DISCLOSURE is a threat where a TA.EXTERNAL or a TA.INSIDER discloses all or part of the private key over logical TOE interface or physical interface of the operational environment by using covert channel mechanisms. This threat is countered by several security objectives. **OE.PRIVATE_KEY_MANAGEMENT** (Secure Management of Private Key) establishes that the TOE environment has to ensure the confidentiality and integrity of the private key. Also, for confidentiality and integrity purposes, the TOE environment has to implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority. In addition, the use of a certified cryptographic module (**OE.CERTIFIED_CM** (Certified cryptographic module)) provides a minimum level of assurance regarding the protection of the private key, diminishing the possibility of an attacker to export the private key from the module. On the other hand, **OE.SECURE_OPER** (Secure Operating Procedures) establishes procedures and controls in the TOE environment to ensure the secure operation of the TOE services, diminishing the possibility of an attacker to implement the adverse action. The physical access to the TOE (**OE.PROTECT_ACCESS** (Prevention of Unauthorized Physical Access)) is also restricted to authorized personnel only, eliminating the possibility of a TA.EXTERNAL to use physical interfaces for the private key disclosure. In the case the cryptographic module used by the TOE supports backup of OCSP private keys, confidentiality of the private key is ensured by **OE.SECURE_BACKUP** (Secure backup of private keys), aimed at establishing personnel, procedurals and technical measures during copy, storage and restoration of private keys. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training) due to the liability issues involved.

T.CRYPTO is a threat where a TA.EXTERNAL or a TA.INSIDER might deduce the private key referred by R.KEY_PAIR_PRIV from the R.KEY_PAIR_PUB or create a forged digital signature due to the use of a weak cryptographic suite by TOE for

either key pair generation or digital signature operation. This threat is directly covered by **O.CRYPTO** (Secure Cryptographic Operations).

T.MISUSE is a threat by which a TA.EXTERNAL or a TA.INSIDER who is able to access the TOE services uses these services without proper authorization or in a manner for which they are not intended. This threat is countered by several security objectives. First, several audit trails recorded by the TOE (**O.AUDIT** (Generation and Export of Audit Data)) and later on reviewed by the auditors (**OE.AUDIT_REVIEW** (Audit review)) permit to monitor the security-sensitive activities undertaken during the usage of the TOE services. In particular, the next events (in brackets) are recorded for each TOE service:

- user management (modification of TOE user management data, adding new users or roles, deleting users or roles)
- OCSP service configuration (changes in the R.OCSP_CONTEXT)
- Time-stamping service configuration (changes in the R.TST_CONTEXT, updates of the internal clock values)
- start of OCSP service operation (TOE initialization, TOE start-up, start of OCSP service operation)
- stop of OCSP service operation (stop of OCSP service operation)
- start of time-stamping service operation (TOE initialization, TOE start-up, start of time-stamping service operation)
- stop of OCSP service operation (stop of OCSP service operation)
- stop of time-stamping service operation (stop of time-stamping service operation)
- key destruction (destruction of R.OCSP_KEY_PAIR_PUB/ R.OCSP_KEY_PAIR_PRIV pairs or R.TST_KEY_PAIR_PUB/ R.TST_KEY_PAIR_PRIV)
- generation of key pair (generation of R.OCSP_KEY_PAIR_PUB/R.OCSP_KEY_PAIR_PRIV or R.TST_KEY_PAIR_PUB/R.TST_KEY_PAIR_PRIV key pairs)
- public key export for certificate request (export of R.OCSP_KEY_PAIR_PUB or R.TST_KEY_PAIR_PUB for certificate request)
- certificate import (OCSP o time-stamping certificates import)
- OCSP responses generation, time-stamping responses generation and internal audit (OCSP responses generation)

Audit related security objectives intend to mitigate the threat where the threat agent is a TA.INSIDER. For threat agents TA.EXTERNAL, this threat is countered by authentication and access control mechanisms implemented by the TOE, and represented by the objectives **O.USER_AUTHENTICATION** (Authentication of TOE Users) and **O.RBAC** (Role-based Access Control to TOE Services) respectively. This threat is also countered by **OE.SECURE_OPER** (Secure Operating Procedures),

which focuses on procedures and controls implemented by the TOE environment towards ensuring a secure operation of the TOE services. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training), which covers the awareness and training of the personnel that use or access the TOE. This objective diminishes the threat in all cases (TA.EXTERNAL or TA.INSIDER) due to the liability issues. OE.ORS sets up an OCSP policy, ensuring that the application, organizational and technical measures are enforced against misuse by TA.EXTERNAL or TA.INSIDER. These measures include prevention, protection and detection measures, such as access control or audit trails review.

T.DATE_AND_TIME_ALTERATION is a threat that represents a TA.INSIDER that changes some information of R.DATE_AND_TIME with the purpose to make the TOE issue signed time-stamps with an intended time that deviates from the actual UTC date and time. The threat details two possible ways of implementing the attack, both of which are meant at modifying the reference time with an arbitrary date. This threat is countered by **O.AUDIT** (Generation and Export of Audit Data), which establishes the need to record events relevant to changes in the values managed by the internal clock, and **OE.AUDIT_REVIEW** (Audit review), which ensures that the auditors regularly check the audit trails and notify in the case that an incident occurs. This threat is diminished by **OE.PERSONNEL** (Liability and Training), reducing the motivation to execute the adverse action due to the liability and legal consequences. Finally, this threat is mitigated by **O.SYNCHRONISATION** (stop of operation under asynchrony with UTC time source), by which no timestamp is issued if the synchronization to the trusted UTC time source is outside the specified limit. This security objective mitigates one of two possible implementation ways of the threat. In particular, case (1), when the TA.INSIDER sets the time of the internal clock with an arbitrary date in the past or in the future that is outside the range of clock accuracy.

T.UNRELIABLE_TST is a threat where the requester of TOE Services receives an unreliable TST. This threat is countered by **O.TST** (Secure Time Stamp Tokens), which states that the TOE shall issue valid Time Stamp Tokens with reliable information to prevent the requester from relying on a bad Token.

T.INSECURE_INITIALISATION is a threat by which a TA.EXTERNAL or a TA.INSIDER initializes the TOE with insecure R.TSF_DATA. This threat is countered by several security objectives. First, audit trails related to TOE initialization are recorded by the TOE (**O.AUDIT** (Generation and Export of Audit Data)) and later on reviewed by the auditors (**OE.AUDIT_REVIEW** (Audit review)). This ensures that any initialization is recorded and appropriately traced back to the corresponding user and date. This threat is also countered by **OE.SECURE_INIT** (Secure Initialization Procedures), which establishes procedures and controls in the TOE environment aimed at ensuring the secure set-up and initialization of the

TOE services. Finally, this threat is diminished by **OE.PERSONNEL** (Liability and Training), which covers the awareness and training of the personnel that use or access the TOE. This objective diminishes the threat due to the liability issues, and also because of the training undertaken.

T.AUDIT_ALTERATION is a threat where a TA.EXTERNAL or TA.INSIDER alters the TOE R.AUDIT_DATA. This threat is countered by **O.AUDIT_PROTECTION** (Protection of audit data), which states that the TOE shall implement mechanisms to prevent a T.EXTERNAL and T.INSIDER from modifying R.AUDIT_DATA.

T.UNRELIABLE_OCSP_RESPONSE is a threat where the requester of TOE Services receives an unreliable OCSP response. This threat is countered by **O.OCSP_R** (Secure OCSP Responses), which states that the TOE shall issue valid OCSP responses with reliable information to prevent the requester from relying on a bad response.

OSP.ALGORITHMS states that the TOE shall use only approved algorithms and algorithm parameters defined as acceptable for the key pair generation (R.OCSP_KEY_PAIR_PUB/R.TST_KEY_PAIR_PUB and private key referred by R.OCSP_KEY_PAIR_PRIV/R.TST_KEY_PAIR_PUB), OCSP responses signing and time-stamping reposes signing. The policy includes the generation of random numbers and the quality of the key pairs generated. The aim is to ensure the confidentiality and integrity of private keys (private key referred by R.OCSP_KEY_PAIR_PRIV and R.TST_KEY_PAIR_PRIV) and the integrity of public keys (R.OCSP_KEY_PAIR_PUB and R.TST_KEY_PAIR_PUB). With this regard, the policy also states that the TOE shall support cryptographic algorithms and key lengths conformant to the rules defined by the relevant national CC Certification Body. This organizational security policy is addressed by several objectives. **O.CRYPTO** (Secure Cryptographic Operations) provides a direct satisfaction of this OSP. Also, as the private key is generated and managed by the OCSP service only, the TOE is required to ensure the integrity of the public key when it is under its control and before it is exported for certification, as defined by **O.PUBLIC_KEY_MANAGEMENT** (Secure Management of Public Key). On the other hand, the TOE environment has to ensure the confidentiality and integrity of the private key (**OE.PRIVATE_KEY_MANAGEMENT** (Secure Management of Private Key)). Both to ensure this and for the key pair generation (**OE.KEY_PAIR_GENERATION** (Public Key/Private Key Pair Generation)), the TOE environment has to implement secure cryptographic algorithms and parameters compliant with the requirements established by the national authority.

OSP.OCSP_SERVICE states that the TOE shall generate OCSP responses in conformity with the OCSP policy, and where the OCSP responses shall be signed using the private key referenced in the R.OCSP_CONTEXT. This organizational security policy is addressed by two security objectives. For the TOE, **O.AUDIT**

(Generation and Export of Audit Data) requires the TOE to audit a number of events, including the OCSP responses generation. For this event some relevant information from the R.OCSP_CONTEXT has to be incorporated (identification of the time source, the OCSP policy and the identifier of the key pair used in the OCSP responses generation process), ensuring that if the OCSP policy is wrongly applied, or a private key different to the one referenced in the R.OCSP_CONTEXT is used, then it will be detected by reviewing the recorded audit trails. For the TOE environment, **OE.AUDIT_REVIEW** (Audit review) mandates the TOE Auditors to check the audit trails on a regular basis, and notify the corresponding authority in the case that an incident occurred.

OSP.OCSP_REQUEST_MGMT states that the OCSP protocol implemented by the TOE shall ensure that the OCSP response is generated in conformity with the data received in the request. The requests, as defined in R.OCSP_REQUEST, include at least the identification of the certificate whose status information is to be obtained. The security objective **OE.OCSPRESPONSE_VERIFICATION** (OCSP response verification) meets this policy by establishing that the requester has to verify the correctness of the responses received from the TOE by verifying the digital signature of the responses and checking if the certificate identification within the received OCSP response is the same as the one included in the corresponding request. Consequently, this allows the requester to check whether the response has been appropriately generated by the TOE according to their request.

A.VAS assumes that the OCSP Response System meets the requirements laid down in [EN319411-2] or equivalent. This assumption is directly covered by **OE.ORS** (Secure OCSP Responses).

A.ACCESS_PROTECTED assumes that the TOE is protected by physical and organizational protection measures implemented by the TOE environment, including restricted physical access to the TOE by authorized persons only and shall require dual control. This assumption is covered by **OE.PROTECT_ACCESS** (Prevention of Unauthorized Physical Access), which establishes that the TOE has to be protected by physical, logical and organizational protection measures implemented by the TOE environment in order to prevent any TOE modification, as well as any protected assets disclosure. This objective includes measures to restrict the TOE usage to authorized persons only and that require dual control.

A.OCSPRESPONSE_VERIFICATION assumes that the requester verifies the correctness of the responses received from the TOE and ensures its preservation, if needed. This assumption is directly covered by **OE.OCSPRESPONSE_VERIFICATION** (OCSP response verification).

A.AUDIT_REVIEW assumes that the TOE Auditors check the audit trails on a regular basis, and notify the corresponding authority in the case that an incident occurred. This assumption is directly covered by **OE.AUDIT_REVIEW** (Audit review).

A.CA assumes that the Certification Authority that issues the certificates to the TOE implements a set of practices in conformity with their CP/CPS. This assumption is directly covered by **OE.CA** (Certification Authority).

A.CERTIFIED_CM assumes that the cryptographic module used by the TOE to digitally sign the response is a certified device as required in EN 319 411-2 or equivalent. This assumption is directly covered by **OE.CERTIFIED_CM** (Certified cryptographic module).

A.SECURE_BACKUP assumes that, in the case the cryptographic module used by the TOE supports backup of OCSP private keys, they are copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see A.ACCESS_PROTECTED). The personnel authorized to carry out this function shall be limited to those requiring to do so under the established practices. The assumption also indicates that any backup copies of the OCSP private signing keys have to be protected by the cryptographic module to ensure its integrity and confidentiality before being stored outside that device. This assumption is directly covered by **OE.SECURE_BACKUP** (Secure backup of private keys).

5 Extended Components Definition

5.1 Extended FCS Components

5.1.1 FCS_TLSC_EXT TLS Client Protocol

Family behaviour

The component in this family addresses the ability for a client to use TLS to protect data between the client and a server using the TLS protocol.

Component levelling

FCS_TLSC_EXT.1 TLS Client Protocol requires that the client side of TLS be implemented as specified.

Management:

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.1.1.1 FCS_TLSC_EXT.1 TLS Client Protocol

Hierarchical to: No other components.

Dependencies: No dependencies

FCS_TLSC_EXT.1.1 The TSF shall implement [selection: TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [selection: Select supported ciphersuites for TLS 1.2 from List 1, Select supported ciphersuites for TLS 1.3 from List 2] and no other ciphersuites.

List 1 - List of supported TLS-related ciphersuites for TLS 1.2: *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268* , *TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 8422, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 8422, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 8422, TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,*

TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268, TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305.

List 2: List of supported TLS-related ciphersuites for TLS 1.3: *TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_AES_128_CCM_SHA256, TLS_AES_128_CCM_8_SHA256, TLS_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305.*

FCS_TLSC_EXT.1.2 The TSF [selection: provides, does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

Application Note 103

The option 'provides' should be selected if the TOE provides the ability to configure the list of ciphers as defined in FCS_TLSC_EXT.1.1 (e.g. enabling/disabling of ciphers, ordering, assigning priorities). Otherwise, the option 'does not provide' should be selected.

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid [selection: without any administrator override mechanism, except with the following administrator override: If the TSF fails to determine the revocation status the TSF shall allow the administrator to provide override authorization to establish the connection on a per certificate basis.].

5.1.2 FCS_TLSS_EXT TLS Server Protocol

Family behaviour

The component in this family addresses the ability for a server to use TLS to protect data between the client and a server using the TLS protocol.

Component levelling

FCS_TLSS_EXT.1 TLS Server Protocol requires that the server side of TLS be implemented as specified.

Management:

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.1.2.1 FCS_TLSS_EXT.1 TLS Server Protocol

Hierarchical to: No other components.

Dependencies: No dependencies

FCS_TLSS_EXT.1.1 The TSF shall implement [selection: TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)] supporting the following ciphersuites: [selection: Select supported ciphersuites for TLS 1.2 from List 1, Select supported ciphersuites for TLS 1.3 from List 2] and no other ciphersuites.

List 1 - List of supported TLS-related ciphersuites for TLS 1.2:
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,
TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 8422,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 8422,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 8422,
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305.

List 2: List of supported TLS-related ciphersuites for TLS 1.3: *TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_AES_128_CCM_SHA256, TLS_AES_128_CCM_8_SHA256, TLS_CHACHA20_POLY1305_SHA256,*
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305,
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using [selection: RSA with key size [selection: 2048, 3072, 4096] bits; ECDSA over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves].

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using: [selection: RSA key establishment with key size [selection: 2048, 3072, 4096] bits; EC Diffie-Hellman key agreement over [selection: NIST curves [selection: secp256r1, secp384r1, secp521r1], Curve25519 (X25519) as defined in RFC 7748] and no other curves;; Diffie-Hellman parameters [selection: of size 2048 bits, of size 3072 bits, of size 4096 bits, of size 6144 bits, of size 8192 bits, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192]].

5.2 Extended FDP Components

5.2.1 FDP_OCSP_EXT OCSP Responses issuance

Family behaviour

OCSP basic responses issued by the TOE shall be compliant with IETF RFC 6960.

Component levelling

FDP_OCSP_EXT OCSP Responses issuance requires that the OCSP responses issued by the TOE be generated as specified.

Management:

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.2.1.1 FDP_OCSP_EXT.1 OCSP Responses issuance

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_OCSP_EXT.1.1 If a TSF is configured to allow OCSP responses of the basic response type, the TSF shall verify that all mandatory fields in the OCSP basic response contain values in accordance with IETF RFC 6960. At a minimum, the following items shall be validated:

1. The `version` field shall contain a 0.

2. If the `issuer` field contains a null Name (e.g., a sequence of zero relative distinguished names), then the response shall contain a critical `issuerAltName` extension.

3. The `signatureAlgorithm` field shall contain the OID for a FIPS-approved digital signature algorithm.

4. The `thisUpdate` field shall indicate the time at which the status being indicated is known to be correct.

5. The `producedAt` field shall indicate the time at which the OCSP responder signed the response.

6. The time specified in the `nextUpdate` field (if populated) shall not precede the time specified in the `thisUpdate` field.

5.2.2 FDP_TST_EXT Time Stamp Tokens issuance

Family behaviour

Time Stamp Tokens issued by the TOE shall be compliant with IETF RFC 3161.

Component levelling

FDP_TST_EXT Time Stamp Tokens issuance requires that the TST responses issued by the TOE be generated as specified.

Management:

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.2.2.1 FDP_TST_EXT.1 Time Stamp Tokens issuance

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_TST_EXT.1.1 The TSF shall verify that all time stamp tokens are issued in accordance with IETF RFC 3161. At a minimum, the following items shall be validated:

1. The `version` field shall contain a 1.

2. The `nonce` field shall be present if it was present in the Time Stamp Request; in such a case, it shall be equal the value provided in the Time Stamp Request structure.

3. The `messageImprint` must have the same value as the similar field in TimeStampReq.

4. The `serialNumber` field must be unique for each `TimeStampToken` issued by a given time-stamping service (i.e., the TSA name and serial number identify a

unique `TimeStampToken`). This property MUST be preserved even after a possible interruption (e.g., crash) of the service.

5. The `genTime` field shall contain the time expressed as UTC time at which the time-stamp token has been created by the time-stamping service.

6 Security Requirements

6.1 Security Functional Requirements

6.1.1 Subjects, objects, operations and security attributes

6.1.1.1 Subjects

We define the following subjects:

- S.OFFICER: Security officer.
- S.REQUESTER: Entity that uses the certificates validation or the time-stamp generation service.
- S.AUDITOR: Auditor.

6.1.1.2 Objects

We define the following list of objects:

- OB.OCSP_CONTEXT: This object corresponds to the R.OCSP_CONTEXT.
- OB.OCSP_RESPONSE: This object corresponds to the R.OCSP_RESPONSE.
- OB.OCSP_REQUEST: This object corresponds to the R.OCSP_REQUEST.
- OB.OCSP_PUB_KEY: This object corresponds to the R.OCSP_KEY_PAIR_PUB.
- OB.OCSP_PRIV_KEY: This object corresponds to the R.OCSP_KEY_PAIR_PRIV.
- OB.TST_CONTEXT: This object corresponds to the R.TST_CONTEXT.
- OB.TST_TOKEN: This object corresponds to the R.TST_TOKEN.
- OB.TST_REQUEST: This object corresponds to the R.TST_REQUEST.
- OB.TST_PUB_KEY: This object corresponds to the R.TST_KEY_PAIR_PUB.
- OB.TST_PRIV_KEY: This object corresponds to the R.TST_KEY_PAIR_PRIV.
- OB. DATE_AND_TIME: This object corresponds to the R.DATE_AND_TIME.
- OB.TLS_CONTEXT: This object corresponds to the R.TLS_CONTEXT.

6.1.1.3 Operations

We define the following operations:

- OP.OCSP_CONTEXT_CREATION: creation of OB.OCSP_CONTEXT, including the request to create a key pair in the HSM.
- OP.OCSP_CONTEXT_DESTRUCTION: destruction of OB.OCSP_CONTEXT.
- OP.OCSP_CONTEXT_MODIFICATION: modification of OB.OCSP_CONTEXT.
- OP.OCSP_CONTEXT_CONSULTATION: consultation of OB.OCSP_CONTEXT.
- OP.OCSP_PUBLIC_KEY_EXPORT: export of OB.OCSP_PUB_KEY to obtain the validation authority certificate.

- OP.OCSP_UNIT_CERTIFICATE_IMPORT: import of the validation authority certificate into OB.OCSP_CONTEXT.
- OP.OCSP_REQUEST_IMPORT: reception of OB.OCSP_REQUEST.
- OP.OCSP_RESPONSE_CREATION: generation of OB.OCSP_RESPONSE.
- OP.OCSP_RESPONSE: sending of OB.OCSP_RESPONSE to S.REQUESTER.
- OP.TST_CONTEXT_CREATION: creation of OB.TST_CONTEXT, including the request to create a key pair in the HSM.
- OP.TST_CONTEXT_DESTRUCTION: destruction of OB.TST_CONTEXT.
- OP.TST_CONTEXT_MODIFICATION: modification of OB.TST_CONTEXT.
- OP.TST_CONTEXT_CONSULTATION: consultation of OB.TST_CONTEXT.
- OP.TST_PUBLIC_KEY_EXPORT: export of OB.TST_PUB_KEY to obtain the time-stamping unit certificate.
- OP.TST_UNIT_CERTIFICATE_IMPORT: import of the time-stamping unit certificate into OB.TXT_CONTEXT.
- OP.TST_TOKEN_REQUEST_IMPORT: reception of OB.TST_REQUEST.
- OP.TST_TOKEN_CREATION: generation of OB.TST_TOKEN.
- OP.TST_TOKEN_RESPONSE: sending of OB.TST_TOKEN to S.REQUESTER.
- OP.INIT_DATE_AND_TIME: initialization of OB.DATE_AND_TIME.
- OP.TLS_CONTEXT_CREATION: creation of OB.TLS_CONTEXT.
- OP.TLS_CONTEXT_DESTRUCTION: destruction of OB.TLS_CONTEXT.
- OP.TLS_CONTEXT_MODIFICATION: modification of OB.TLS_CONTEXT

6.1.1.4 Security attributes

For each object, we define a list of security attributes:

OB.OCSP_CONTEXT

- AT.OCSP_CONTEXT_OPERATIONAL: This attribute indicates if the OCSP service context is operational or not.
- AT.OPERATIONAL_OCSP_CONTEXT_COMPLETE: This attribute indicates that all the information needed to create the OCSP service operational context has been filled in.
- AT.NON_OPERATIONAL_OCSP CONTEXT_KEY_PAIR_CREATED: This attribute indicates that the key pair associated with the OCSP service context has been created.
- AT.OCSP_POLICY: This attribute describes the OCSP policy that will be used to generate the OCSP responses.
- AT.OCSP_IMPORTED_CERTIFICATE: Value of the OCSP certificate imported into the TOE.
- AT.IMPORTED_OCSP_CERTIFICATE_PUBLIC_KEY: value of the public key of the non operational OCSP service context into which the certificate is imported.

- AT.NON_OPERATIONAL_OCSP_CONTEXT_PRIVATE_KEY: value of reference to the private key of the non operational OCSP service context into which the certificate is imported.
- AT.OCSP_PUBLIC_KEY_ALGORITHM_IDENTIFIER: value of the public key algorithm identifier of the OCSP service certificate.

OB.TST_CONTEXT

- AT.TST_CONTEXT_OPERATIONAL: This attribute indicates if the time-stamp service context is operational or not.
- AT.OPERATIONAL_TST_CONTEXT_COMPLETE: This attribute indicates that all the information needed to create the operational time-stamp service context has been filled in.
- AT.NON_OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED: This attribute indicates that the key pair associated with the time-stamp service context has been created.
- AT.MONOTONIC_TIMESTAMP_TOKEN_TIME: This attribute indicates if the time included in the last issued time-stamp token is greater or equal than the one in the preceding one.
- AT.TST_PRIVATE_KEY_EFFECTIVE_VALIDITY_PERIOD: This attribute indicates the expiration date of the certificate associated with the private key of the time-stamp service.
- AT.DEFAULT_TST_POLICY: This attribute describes the default time-stamp policy associated with the context.
- AT.TST_IMPORTED_CERTIFICATE: Value of the time-stamping certificate imported into the TOE.
- AT.IMPORTED_TST_CERTIFICATE_PUBLIC_KEY: value of the public key of the non operational context into which the time-stamp service certificate is imported.
- AT.NON_OPERATIONAL_TST_CONTEXT_PRIVATE_KEY: value of reference to the private key of the non operational time-stamp service context into which the certificate is imported.
- AT.TST_IMPORTED_CERTIFICATE_PRIVATE_KEY_VALIDITY_PERIOD: value of the private key validity period contained in the time-stamp service certificate imported into the TOE, if present.
- AT.TST_PUBLIC_KEY_ALGORITHM_IDENTIFIER: value of the public key algorithm identifier of the time-stamp service certificate.

OB.TLS_CONTEXT

- AT.TLS_IMPORTED_PRIV_KEY: Value of the Auditor UI (Grafana) HTTPS (TLS) private key.

- AT.TLS_IMPORTED_CERTIFICATE: Value of the Auditor UI (Grafana) HTTPS (TLS) certificate imported into the TOE.
- AT.TLS_SIEM_CERTIFICATE: Value of the certificate imported into the TOE to to validate the HTTPS (TLS) connection with the SIEM.

OB.OCSP_RESPONSE

- AT.OCSP_RESPONSE_VALUE: value of the OCSP response.

OB.OCSP_REQUEST

- AT.OCSP_REQUEST_VALUE: value of the OCSP request.
- AT.OCSP_REQUEST_NONCE: value of the `nonce` contained in the imported OCSP request, if present.

OB.OCSP_PUB_KEY

- AT.OCSP_PUBLIC_KEY_VALUE: value of the public key of the OCSP service certificate.

OB.OCSP_PRIV_KEY

- AT.OCSP_PRIVATE_KEY_VALUE: value of reference to the private key of the OCSP service.

OB.TST_TOKEN

- AT.TST_TOKEN_TIME: value of the time contained in the exported timestamp token
- AT.TST_UNIT_CERTIFICATE_REFERENCE: value of the certificate reference
- AT.USED_TST_POLICY_IDENTIFIER: value of the time-stamping policy identifier contained in the exported timestamp token
- AT.TST_TOKEN_SIGNATURE: value of the digital signature of the timestamp token.

OB.TST_REQUEST

- AT.TST_TOKEN_REQUEST: Value of the imported timestamp token request.
- AT.HASH_ALGORITHM_IDENTIFIER: Value of the hash algorithm identifier used to generate the data imprint contained in the imported timestamp token request.
- AT.DATA_IMPRINT: value of the data imprint contained in the imported timestamp token request.
- AT.REQUEST_POLICY_IDENTIFIER: value of the time-stamping policy identifier contained in the imported timestamp token request, if present
- AT.TST_REQUEST_NONCE: value of the `nonce` contained in the imported timestamp token request, if present.

OB.TST_PUB_KEY

- AT.PUBLIC_KEY_VALUE: value of the public key of the time-stamp service certificate.

OB.PRIV_KEY

- AT.PRIVATE_KEY_VALUE: value of reference to the private key of the time-stamp service.

OB. DATE_AND_TIME

- AT.DATE_AND_TIME_VALUE: This attribute indicates the clock value used by the context.
- AT.DATE_AND_TIME_SYNCHRONIZED: This attribute indicates that the date and time value used by the context is synchronized with UTC.

6.1.2 Security requirement operations

Common Criteria allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in Part 1 of CC. Each of these operations is used in this PP as follows:

- A refinement operation is used to add detail to a requirement, and thus further restricts a requirement. A refinement of a security requirement is included in text as *italicized and underlined* text. In cases where words from a CC requirement were deleted, the deleted text appears ~~crossed out~~.
- A selection operation is used to select one or more options provided by the CC in stating a requirement. A selection is indicated in square brackets with selected option as underlined text, italicized and in blue colour [selection: *minimum*]. Selections left to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, and with the available options italicized and in blue colour [selection: *minimum, basic, detailed, not specified*].
- An assignment operation is used to assign a specific value to an unspecified parameter. An assignment is indicated in square brackets with the specific value as underlined text, italicized and in blue colour [assignment: *none*]. Assignments left to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made, and with the original text italicized and in blue colour [assignment: *other audit relevant information*].
- An iteration operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.1.3 User Data Protection (FDP)

FDP_ACC.1/Context_Management_Policy Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control.

FDP_ACC.1.1 The TSF shall enforce the [assignment: *context management policy*] on [assignment:

- *Subjects: subject representing the Security Officer (S.OFFICER),*
- *Objects: OCSP contexts (OB.OCSP_CONTEXT), Time-stamp contexts (OB.TST_CONTEXT),*

Operations: creation, modification, destruction and consultation of the OCSP contexts (OP.OCSP_CONTEXT_CREATION, OP.OCSP_CONTEXT_MODIFICATION, OP.OCSP_CONTEXT_DESTRUCTION, and OP.OCSP_CONTEXT_CONSULTATION respectively).] and creation, modification, destruction and consultation of the time-stamping contexts (OP.TST_CONTEXT_CREATION, OP.TST_CONTEXT_MODIFICATION, OP.TST_CONTEXT_DESTRUCTION, and OP.TST_CONTEXT_CONSULTATION respectively).].

FDP_ACF.1/Context_Management_Policy Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization.

FDP_ACF.1.1 The TSF shall enforce the [assignment: *context management policy*] to objects based on the following: [assignment:

- *Objects: OB.OCSP_CONTEXT, OB.TST_CONTEXT*
- *SFP-relevant security attributes: AT.OCSP_CONTEXT_OPERATIONAL, AT.OPERATIONAL_OCSP_CONTEXT_COMPLETE, AT.NON_OPERATIONAL_OCSP_CONTEXT_KEY_PAIR_CREATED], AT.TST_CONTEXT_OPERATIONAL, AT.OPERATIONAL_TST_CONTEXT_COMPLETE and AT.NON_OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED].*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- *The creation of a OCSP service context (OP.OCSP_CONTEXT_CREATION) is authorized to be performed only by an authenticated Security Officer (S.OFFICER)*
- *The consultation of the following information only that are contained in both non operational and operational OCSP service contexts*

(OP.OCSP_CONTEXT_CONSULTATION) is authorized to be performed only by an authenticated Security Officer (S.OFFICER):

- *OCSP policy.*
- *The OCSP unit certificate (for operational contexts only).*

- *The modification of all information contained in a OCSP service context except the key pair value (OP.OCSP_CONTEXT_MODIFICATION) is authorized to be performed only by an authenticated Security Officer (S.OFFICER).*
- *The destruction of both non operational and operational OCSP service contexts (OP.OCSP_CONTEXT_DESTRUCTION) is authorized to be performed by an authenticated Security Officer (S.OFFICER)].*
- *The creation of a time-stamp service context (OP.TST_CONTEXT_CREATION) is authorized to be performed only by an authenticated Security Officer (S.OFFICER)*
- *The consultation of the following information only that are contained in both non operational and operational timestamp service contexts (OP.TST_CONTEXT_CONSULTATION) is authorized to be performed only by an authenticated Security Officer (S.OFFICER):*
  - *the accuracy with UTC time that is guaranteed for the time contained in time-stamping tokens.*
  - *reference(s) of accepted time-stamping policies.*
  - *identifier(s) of authorized hash algorithms or each time-stamping Policy (recommendations for the choice of hash algorithms are provided by national authority).*
  - *the time-stamping unit certificate (for operational contexts only).*
- *The modification of all information contained in a time-stamp service context except the key pair value (OP.TIMESTAMPCONTEXT_MODIFICATION) is authorized to be performed only by an authenticated Security Officer (S.OFFICER).*
- *The destruction of both non operational and operational time-stamp service contexts (OP.TST_CONTEXT_DESTRUCTION) is authorized to be performed by an authenticated Security Officer (S.OFFICER)].*

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

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment:

- *The Auditor (S.AUDITOR) cannot perform the following operations:*
  - *creation of OB.OCSP_CONTEXT (OP.OCSP_CONTEXT_CREATION)*
  - *destruction of OB.OCSP_CONTEXT (OP.OCSP_CONTEXT_DESTRUCTION)*
  - *modification of OB.OCSP_CONTEXT (OP.OCSP_CONTEXT_MODIFICATION)]*

- *consultation of OB.OCSP_CONTEXT (OP.OCSP_CONTEXT_CONSULTATION)*
- *creation of OB.TST_CONTEXT (OP.TST_CONTEXT_CREATION)*
- *destruction of OB.TST_CONTEXT (OP.TST_CONTEXT_DESTRUCTION)*
- *modification of OB.TST_CONTEXT (OP.TST_CONTEXT_MODIFICATION)]*
- *consultation of OB.TST_CONTEXT (OP.TST_CONTEXT_CONSULTATION)*

FDP_ITC.1/Context_Management_Policy Import of user data without security attributes

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_MSA.3 Static attribute initialization

FDP_ITC.1.1 The TSF shall enforce the [assignment: *context management policy*] when importing user data, controlled under the SFP, from outside of the TOE.

Application Note: The imported user data correspond to the following information involved during the operations of creation and modification of OCSP contexts:

- *configuration of the database to be used for storing the certificate information,*
- *configuration of the HSM to be used for storing the OCSP key pairs,*
- *identification and configuration of the certificate source that shall be used to obtain the certificates and/or certificate status changes for a Certification Authority,*
- *identifier of the OCSP policy to be used for generating OCSP responses.*

The imported user data correspond to the following information involved during the operations of creation and modification of timestamping contexts:

- *identification of the time source that shall be used to obtain the time value contained in timestamp tokens,*
- *accuracy with UTC time that is guaranteed for the time contained in timestamping tokens,*
- *reference(s) of accepted timestamping policies,*
- *identifier(s) of authorized hash algorithms for each timestamping policy.*

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

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

FDP_ITC.2/Context_Management_Policy Import of user data with security attributes

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1 The TSF shall enforce the [assignment: *context management policy*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 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 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 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *none*].

FDP_ETC.1/*Non_Operational_Context_Public_Key Export of user data without security attributes*

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control].

FDP_ETC.1.1 The TSF shall enforce the [assignment: *key management policy*] when exporting user data, controlled under the SFP(s), outside of the TOE.

Application Note: The exported user data are the public keys of non operational OCSP and time-stamp service contexts which are generated by the TOE during the respective context creation phase along with the corresponding public key algorithm identifiers.

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

FDP_ITC.2/OCSP_And_Timestamp_unit_Certificate Import of user data with security attributes

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path], FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1 The TSF shall enforce the [assignment: *key management policy*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 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 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 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *none*].

FDP_IFC.1/Key_Management_Policy Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [assignment: *key management policy*] on [assignment:

- *Information:*
  - *value of the OCSP certificate imported into the TOE (AT.OCSP_IMPORTED_CERTIFICATE),*
  - *value of the public key contained in the OCSP unit certificate imported into the TOE (AT.IMPORTED_OCSP_CERTIFICATE_PUBLIC_KEY),*
  - *value of the public key of the non operational context into which the certificate is imported (AT.OCSP_PUBLIC_KEY_VALUE),*
  - *value of reference to the private key of the non operational context into which the certificate is imported (AT.OCSP_PRIVATE_KEY_VALUE),*
  - *value of the public key algorithm identifier (AT.OCSP_PUBLIC_KEY_ALGORITHM_IDENTIFIER).*
  - *value of the time-stamping unit certificate imported into the TOE (AT.TST_IMPORTED_CERTIFICATE),*
  - *value of the public key contained in the time-stamping unit certificate imported into the TOE (AT.TST_IMPORTED_CERTIFICATE_PUBLIC_KEY),*
  - *value of the public key of the non operational context into which the certificate is imported (AT.TST_PUBLIC_KEY_VALUE),*

  - *value of reference to the private key of the non operational context into which the certificate is imported (AT.TST_PRIVATE_KEY_VALUE),*
  - *value of the public key algorithm identifier (AT.TST_PUBLIC_KEY_ALGORITHM_IDENTIFIER).*
- *Subjects:*
  - *Security Officer (S.OFFICER).*
- *Operations:*
  - *export of the public key to obtain the OCSP unit certificate (OP.OCSP_PUBLIC_KEY_EXPORT),*
  - *import of the OCSP unit certificate (OP.OCSP_UNIT_CERTIFICATE_IMPORT).*
  - *export of the public key to obtain the time-stamping unit certificate (OP.TST_PUBLIC_KEY_EXPORT),*
  - *import of the time-stamping unit certificate (OP.TST_UNIT_CERTIFICATE_IMPORT).*
  -
- *Objects:*
  - *OCSP context (OB.OCSP_CONTEXT),*
  - *OCSP key pair (OB.OCSP_PUB_KEY and OB.OCSP_PRIV_KEY)].*
  - *time-stamping contexts (OB.TST_CONTEXT),*
  - *time-stamping key pair (OB.TST_PUB_KEY and OB.TST_PRIV_KEY)].*

FDP_IFF.1/Key_Management_Policy Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control, FMT_MSA.3 Static attribute initialization.

FDP_IFF.1.1 The TSF shall enforce the [assignment: key management policy] based on the following types of subject and information security attributes: [assignment:

- *the security attributes AT.OPERATIONAL_OCSP_CONTEXT_COMPLETE and AT.NON_OPERATIONAL_OCSP_CONTEXT_KEY_PAIR_CREATED associated with a non operational context (OB.OCSP_CONTEXT with security attribute AT.CONTEXT_OPERATIONAL being "False") that indicate respectively if the non operational context is complete (i.e., all required information are specified) and if the key pair has been created by the Security Officer,*
- *the security attribute AT.OCSP_CONTEXT_OPERATIONAL that indicates that a OCSP context (OB.OCSP_CONTEXT) is operational following the authorized import of the OCSP unit certificate.*].
- *the security attributes AT.OPERATIONAL_TST_CONTEXT_COMPLETE and AT.NON_OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED associated with a non operational context (OB.TST_CONTEXT with security attribute*

AT.TST_CONTEXT_OPERATIONAL being "False") that indicate respectively if the non operational context is complete (i.e., all required information are specified) and if the non operational context has been created by the Security Officer,

- *the security attribute AT.TST_CONTEXT_OPERATIONAL that indicates that a time-stamping context (OB.TST_CONTEXT) is operational following the authorized import of the time-stamping unit certificate.*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment:

- *the operation OP.OCSP_PUBLIC_KEY_EXPORT enables the export of the public key of a non operational context and the identifier of the public key algorithm (AT.OCSP_PUBLIC_KEY_VALUE and AT.OCSP_PUBLIC_KEY_ALGORITHM_IDENTIFIER) from the non operational context (OB.OCSP_CONTEXT with security attributes AT.OCSP_CONTEXT_OPERATIONAL being "False" and AT.NON_OPERATIONAL_OCSP_CONTEXT_KEY_PAIR_CREATED being "True") by the subject that exports the public key (S.OFFICER). This operation is authorized to be performed only on behalf of an authenticated Security Officer,*
- *the operation OP.OCSP_UNIT_CERTIFICATE_IMPORT enables the import of the certificate corresponding to the exported public key (AT.IMPORTED_OCSP_CERTIFICATE) into the non-operational context (OB.OCSP_CONTEXT with security attribute AT.OCSP_CONTEXT_OPERATIONAL being "False") by the subject that imports the certificate (S.OFFICER) in order to create the corresponding operational context (OB.OCSP_CONTEXT with security attribute AT.OCSP_CONTEXT_OPERATIONAL being "True"). This operation is authorized to be performed only on behalf of an authenticated Security Officer only if the following conditions hold:*
  - *the non operational context is both complete and created (the value of the security attributes AT.OPERATIONAL_OCSP_CONTEXT_COMPLETE and AT.NON_OPERATIONAL_OCSP_CONTEXT_KEY_PAIR_CREATED are both "True"),*
  - *the value of the public key of the imported certificate (AT.IMPORTED_OCSP_CERTIFICATE_PUBLIC_KEY) corresponds to the value of the public key of the non-operational context into which the OCSP certificate is imported (AT.PUBLIC_OCSP_KEY_VALUE)].*
- *the operation OP.TST_PUBLIC_KEY_EXPORT enables the export of the public key of a non operational context and the identifier of the public key algorithm (AT.TST_PUBLIC_KEY_VALUE and AT.TST_PUBLIC_KEY_ALGORITHM_IDENTIFIER) from the non operational context (OB.TST_CONTEXT with security attributes*

AT.TST_CONTEXT_OPERATIONAL being "False" and AT.TST_NON_OPERATIONAL_CONTEXT_KEY_PAIR_CREATED being "True") by the subject that exports the public key (S.OFFICER). This operation is authorized to be performed only on behalf of an authenticated Security Officer,

- *the operation OP.TST_UNIT_CERTIFICATE_IMPORT enables the import of the certificate corresponding to the exported public key (AT.TST_IMPORTED_CERTIFICATE) into the non operational context (OB.TST_CONTEXT with security attribute AT.TST_CONTEXT_OPERATIONAL being "False") by the subject that imports the certificate (S.OFFICER) in order to create the corresponding operational context (OB.TST_CONTEXT with security attribute AT.TST_CONTEXT_OPERATIONAL being "True"). This operation is authorized to be performed only on behalf of an authenticated Security Officer only if the following conditions hold:*
  - *the non operational context is both complete and created (the value of the security attributes AT.OPERATIONAL_TST_CONTEXT_COMPLETE and AT.NON_OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED are both "True"),*
  - *the value of the public key of the imported certificate (AT.IMPORTED_TST_CERTIFICATE_PUBLIC_KEY) corresponds to the value of the public key of the non operational context into which the time-stamping certificate is imported (AT.TST_PUBLIC_KEY_VALUE)].*

FDP_IFF.1.3 The TSF shall enforce the [assignment: *none*].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [assignment:

- *OCSP certificate (AT.IMPORTED_OCSP_CERTIFICATE) shall be imported into a non-operational context (OB.OCSP_CONTEXT with security attribute AT.OCSP_CONTEXT_OPERATIONAL being "False") whose key pair has been created (AT.NON_OPERATIONAL_OCSP_CONTEXT_KEY_PAIR_CREATED is "True")].*
- *Timestamp Unit certificate (AT.TST_IMPORTED_CERTIFICATE) shall be imported into a non-operational context (OB.TST_CONTEXT with security attribute AT.TST_CONTEXT_OPERATIONAL being "False") whose key pair has been created (AT.NON_OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED is "True")].*
- *Destruction of the time-stamp private key of an operational context if the associated effective private key validity period (AT.TST_PRIVATE_KEY_EFFECTIVE_VALIDITY_PERIOD) has expired*

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment:

- *OCSP certificate (AT.IMPORTED_OCSP_CERTIFICATE) shall not be imported into an operational context (OB.OCSP_CONTEXT with security attribute AT.OCSP_CONTEXT_OPERATIONAL being "True")]*
- *time-stamping certificates (AT. IMPORTED_TST_CERTIFICATE) shall not be imported into an operational context (OB.TST_CONTEXT with security attribute AT.TST_CONTEXT_OPERATIONAL being "True")*

FDP_ACC.1/OCSP_Response_Generation_Policy Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment*: OCSP response generation policy*] on [assignment:

- *Subjects: none*
- *Objects:*
  - *operational contexts (OB.OCSP_CONTEXT with security attribute AT.OCSP_CONTEXT_OPERATIONAL being "True") generating OCSP responses signed against the context signature private key, the value of the OCSP unit certificate reference (AT.IMPORTED_OCSP_CERTIFICATE_PUBLIC_KEY) and the value of the used OCSP policy (AT.OCSP_POLICY),*
  - *generated OCSP responses (OB.OCSP_RESPONSE) containing the information present in the corresponding OCSP requests (OB.OCSP_REQUEST),*
- *Operations: creation and sending of OCSP responses (OP.OCSP_RESPONSE_CREATION and OP.OCSP_RESPONSE)*].

FDP_ACF.1/OCSP_Response_Generation_Policy Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [assignment: *OCSP response generation policy*] to objects based on the following: [assignment:

- *Objects: OB.OCSP_CONTEXT*
- *SFP-relevant security attributes:*

- *the security attribute AT.OCSP CONTEXT OPERATIONAL that indicates if the OCSP context (OB.OCSP_CONTEXT) whose information are used to generate the OCSP response is operational,*
- *the global security attribute AT.OCSP POLICY DEFINED that indicates if an OCSP policy has been defined for the OCSP system using a policy identifier by an authenticated Security Officer*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- *the creation of OCSP responses (OP.OCSP RESPONSE CREATION on OB.OCSP_RESPONSE) is authorized to be performed only in an automatic way by the TOE if the context whose information are used to generate the OCSP response is operational (the security attribute AT.OCSP CONTEXT OPERATIONAL associated with OB.OCSP CONTEXT is "True"),*
- *the signature of OCSP response (OP.OCSP RESPONSE SIGNATURE on OB.OCSP_RESPONSE) is authorized to be performed only in an automatic way by the TOE if the context whose information are used to generate the OCSP response is operational (the security attribute AT.OCSP CONTEXT OPERATIONAL associated with OB.OCSP CONTEXT is "True")*].

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

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

FDP_OCSP_EXT.1 /OCSP Responses issuance

Dependencies: No dependencies

FDP_OCSP_EXT.1.1 If a TSF is configured to allow OCSP responses of the basic response type, the TSF shall verify that all mandatory fields in the OCSP basic response contain values in accordance with IETF RFC 6960. At a minimum, the following items shall be validated:

1. The version field shall contain a 0.

2. If the issuer field contains a null Name (e.g., a sequence of zero relative distinguished names), then the response shall contain a critical `issuerAltName` extension.

3. The `signatureAlgorithm` field shall contain the OID for a FIPS-approved digital signature algorithm.

4. The `thisUpdate` field shall indicate the time at which the status being indicated is known to be correct.

5. The `producedAt` field shall indicate the time at which the OCSP responder signed the response.

6. The time specified in the `nextUpdate` field (if populated) shall not precede the time specified in the `thisUpdate` field.

FDP_ITC.1/Date_and_Time Import of user data without security attributes

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_MSA.3 Static attribute initialization.

FDP_ITC.1.1 The TSF shall enforce the [assignment: *timestamp token generation policy*] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: *additional importation control rules*]

FDP_ACC.1/Timestamp_Token_Generation_Policy Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [assignment*: timestamp token generation policy*] on [assignment:

- *Subjects: none*
- *Objects:*
  - *operational contexts (OB.TST_CONTEXT with security attribute AT.TST_CONTEXT_OPERATIONAL being "True") generating timestamp tokens signed against the context signature private key, the value of the time-stamping unit certificate reference (AT.IMPORTED_TST_CERTIFICATE_PUBLIC_KEY) and the value of the used time-stamping policy (AT.DEFAULT_TST_POLICY),*

  - *generated timestamp tokens (OB.TST_TOKEN) containing the information present in the corresponding timestamp token requests (OB.TST_REQUEST),*
  - *the internal clock (OB. DATE_AND_TIME) with the time value provided by the used internal clock (AT. DATE_AND_TIME_VALUE),*
- *Operations: creation and sending of timestamp tokens (OP.TST_TOKEN_CREATION and OP.TST_TOKEN_RESPONSE)*].

FDP_ACF.1/Timestamp_Token_Generation_Policy Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control, FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [assignment: *timestamp token generation policy*] to objects based on the following: [assignment:

- *Objects: OB.TST_CONTEXT*
- *SFP-relevant security attributes:*
  - *the security attribute AT.TST_CONTEXT_OPERATIONAL that indicates if the time-stamping context (OB.TST_CONTEXT) whose information are used to generate the timestamp token is operational,*
  - *the security attribute AT.TST_PRIVATE_KEY_EFFECTIVE_VALIDITY_PERIOD associated with the used operational context (OB.TST_CONTEXT with security attribute AT.TST_CONTEXT_OPERATIONAL being "True") that indicates the validity period of the context private key,*
  - *the security attribute AT.MONOTONIC_TIMESTAMP_TOKEN_TIME associated with the used operational context (OB.TST_CONTEXT) that indicates if the time value provided by the used internal clock for the current timestamp token is greater or equal to the time value placed in the previous timestamp token generated by this time-stamping context,*
  - *the security attribute AT.DATE_AND_TIME_SYNCHRONIZED associated with the used operational context (OB.TST_CONTEXT with security attribute AT.TST_CONTEXT_OPERATIONAL being "True") that indicates if the internal clock is synchronized with UTC with the accuracy specified in the operational context,*
  - *the global security attribute AT.DEFAULT_TST_POLICY_DEFINED that indicates if a default time-stamping policy has been defined for the time-stamping system using a policy identifier by an authenticated Security Officer*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment:

- *the creation of timestamp tokens (OP.TST_TOKEN_CREATION on OB.TST_TOKEN) is authorized to be performed only in an automatic way by the TOE if the following conditions hold:*
  - *the context whose information are used to generate the timestamp token is operational (the security attribute AT.TST_CONTEXT_OPERATIONAL associated with OB.TST_CONTEXT is "True"),*
  - *the context whose information are used to generate the timestamp token supports the time-stamping policy specified in the token request or the default time-stamping policy when no time-stamping policy has been specified in the token request (the global security attribute AT.DEFAULT_TST_POLICY is defined),*
  - *the used internal clock is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.DATE_AND_TIME_SYNCHRONIZED is "True"),*
- *the signature of timestamp tokens (OP.TST_TOKEN_SIGNATURE on OB.TST_TOKEN) is authorized to be performed only in an automatic way by the TOE if the following conditions hold:*
  - *the context whose information are used to generate the timestamp token is operational (the security attribute AT.TST_CONTEXT_OPERATIONAL associated with OB.TST_CONTEXT is "True"),*
  - *the context private key used to generate the signature of the timestamp token is valid (the date and time of the signature generation is included in the private key validity period defined by the security attribute AT.TST_PRIVATE_KEY_EFFECTIVE_VALIDITY_PERIOD associated with the operational context),*
  - *the internal clock is synchronized with UTC with the accuracy defined in the used operational context (the security attribute AT.DATE_AND_TIME_SYNCHRONIZED is "True")*].

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

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

FDP_TST_EXT.1 /Time Stamp Tokens issuance

Dependencies: No dependencies

FDP_TST_TST.1.1 The TSF shall verify that all time stamp tokens are issued in accordance with IETF RFC 3161. At a minimum, the following items shall be validated:

1. The version field shall contain a 1.

2. The `nonce` field shall be present if it was present in the Time Stamp Request; in such a case, it shall be equal the value provided in the Time Stamp Request structure.

3. The `messageImprint` must have the same value as the similar field in TimeStampReq.

4. The `serialNumber` field must be unique for each `TimeStampToken` issued by a given time-stamping service (i.e., the TSA name and serial number identify a unique `TimeStampToken`). This property MUST be preserved even after a possible interruption (e.g., crash) of the service.

5. The `genTime` field shall contain the time expressed as UTC time at which the time-stamp token has been created by the time-stamping service.

6.1.4 Security Management (FMT)

FMT_MSA.1/Context_Management_Policy Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *context management policy*] to restrict the ability to [selection: *query and modify*] the security attributes [assignment: *AT.OPERATIONAL_OCSP_CONTEXT_COMPLETE, AT.NON_OPERATIONAL_CONTEXT_OCSP_KEY_PAIR_CREATED, and AT.OCSP_CONTEXT_OPERATIONAL, AT.OPERATIONAL_TST_CONTEXT_COMPLETE, AT.NON_OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED and AT.TIME_STAMP_CONTEXT_OPERATIONAL*] to [assignment: *Security Officer (S.OFFICER)*].

Application Note: The modification operation on the security attributes AT.OPERATIONAL_OCSP_CONTEXT_COMPLETE, AT.OCSP_CONTEXT_OPERATIONAL, AT.OPERATIONAL_TST_CONTEXT_COMPLETE, AT.TST_CONTEXT_OPERATIONAL is performed indirectly by the Security Officer (S.OFFICER), since these attribute modifications result from operations performed by the S.OFFICER

(OP.OCSP_CONTEXT_CREATION, OP.OCSP_UNIT_CERTIFICATE_IMPORT, OP.TST_CONTEXT_CREATION and OP.TST_UNIT_CERTIFICATE_IMPORT).

FMT_MSA.1/Multiple_OCSP_Policies Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *context management policy, key management policy, OCSP response generation policy*] to restrict the ability to [selection: *query and modify*] the security attributes [assignment: *AT.OPERATIONAL_OCSP_CONTEXT_COMPLETE, AT.NON_OPERATIONAL_OCSP_CONTEXT_KEY_PAIR_CREATED, AT.OCSP_CONTEXT_OPERATIONAL, AT.OCSP_PRIVATE_KEY_VALUE, AT.OCSP_PUBLIC_KEY_VALUE, AT.OCSP_PUBLIC_KEY_ALGORITHM_IDENTIFIER, AT.NON_OPERATIONAL_OCSP_CONTEXT_PRIVATE_KEY, AT._IMPORTED_OCSP_CERTIFICATE_PUBLIC_KEY, AT.IMPORTED_OCSP_CERTIFICATE, AT.OCSP_POLICY*] to [assignment: *none*].

FMT_MSA.1/Multiple_Timestamping_Policies Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *context management policy, key management policy, timestamp token generation policy*] to restrict the ability to [selection: *query and modify*] the security attributes [assignment: *AT.OPERATIONAL_TST_CONTEXT_COMPLETE, AT.NON_OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED, AT.TST_CONTEXT_OPERATIONAL, AT.TST_PRIVATE_KEY_VALUE, AT.TST_PUBLIC_KEY_VALUE, AT.TST_PUBLIC_KEY_ALGORITHM_IDENTIFIER, AT.NON_OPERATIONAL_TST_CONTEXT_PRIVATE_KEY, AT.IMPORTED_TST_CERTIFICATE_PUBLIC_KEY, AT.IMPORTED_TST_CERTIFICATE, AT.MONOTONIC_TIMESTAMP_TOKEN_TIME*] to [assignment: *none*].

Application Note: The value of the security attribute AT.MONOTONIC_TIMESTAMP_TOKEN_TIME is set to the "True" value by the TOE to enable the first timestamp token to be generated by an operational context.

FMT_MSA.3/Context_Management_Policy Static attribute initialization

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: *context management policy*] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *none*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/Context_Management_Policy Specification of Management Functions

Dependencies: No dependencies.

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

- *modification and query of the following security attributes:*
  - *AT.OPERATIONAL_OCSP_CONTEXT_COMPLETE*
  - *AT.NON_OPERATIONAL_OCSP_CONTEXT_KEY_PAIR_CREATED*
  - *AT.OCSP_CONTEXT_OPERATIONAL*
  - *AT.OPERATIONAL_TST_CONTEXT_COMPLETE*
  - *AT.NON_OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED*
  - *AT.TST_CONTEXT_OPERATIONAL*
  - *AT.MONOTONIC_TIMESTAMP_TOKEN_TIME*].

FMT_MSA.1/Date_and_Time Management of security attributes

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [assignment: *timestamp token generation policy*] to restrict the ability to [selection: query and modify] the security attributes [assignment: *AT.DATE_AND_TIME_SYNCHRONIZED*] to [assignment: *Security Officer (S.OFFICER)*].

FMT_MSA.3/Date_and_Time Static attribute initialization

Dependencies: FMT_MSA.1 Management of security attributes, FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [assignment: timestamp token generation policy] to provide [selection: *restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *Security Officer (S.OFFICER)*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/Date_and_Time Specification of Management Functions

Dependencies: No dependencies.

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

- *query the security attribute AT. DATE_AND_TIME_SYNCHRONIZED,*
- *set the security attribute AT. DATE AND TIME SYNCHRONIZED to "Synchronized" if the internal clock is synchronized with UTC with the accuracy defined in the used operational context,*
- *set the security attribute AT. DATE AND TIME SYNCHRONIZED to "Not synchronized" if the internal clock is not synchronized with UTC with the accuracy defined in the used operational context,*
- *synchronize the internal clock of a time-stamping unit,*
- *periodically compare the time difference between the internal clock of a time-stamping unit with UTC: if the time difference is greater than the authorized value AT.DATE_AND_TIME_SYNCHRONIZED is set to "Not synchronized",*
- *periodically record the time difference between the internal clock of a time-stamping unit with UTC to create and update a log of those time differences,*
- *periodically verify the synchronization of the internal clock of a time-stamping unit by making use of the history of time differences between this internal clock and UTC: if the history of the time differences is not in conformance with the drift authorized over a given time period then AT. DATE_AND_TIME_SYNCHRONIZED is set to "Not synchronized",*
- *initialize the internal clock during the initialization phase of a time-stamping unit by synchronizing it with UTC*.]

Application Note: Period of comparison, authorized value, and length of the time difference history shall be set to meet the requirements of [EN319421] or equivalent.

FMT_MTD.1/Date_and_Time Management of TSF data

Dependencies: FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: [assignment: *initialize (OP.INIT_DATE_AND_TIME)]*] the [assignment: *internal clock of a time-stamping unit (OB.DATE_AND_TIME)*] to [assignment: *Security Officer (S.OFFICER)*].

FMT_SMF.1/Temporary_Interruption Specification of Management Functions

Dependencies: No dependencies.

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

- *supervision of the synchronization of the TOE,*
- *interruption of the time-stamping service in the following cases: the state of the internal clock is "Not synchronized" for the operational context used to generate timestamp tokens (i.e., the security attribute AT.DATE_AND_TIME_SYNCHRONIZED is "False")*]

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *Security Officer (S.OFFICER) and Auditor (S.AUDITOR)*].

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

6.1.5 Protection of the TSF (FPT)

FPT_TDC.1/OCSP_Unit_Certificate Inter-TSF basic TSF data consistency

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: fields of the imported OCSP unit certificates] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [assignment: *the value of the OCSP public key contained in the imported OCSP certificate to verify it corresponds to the value of the non operational OCSP context public key generated during the OCSP context creation phase*] when interpreting the TSF data from another trusted IT product.

FPT_STM.1 Reliable time stamps

Dependencies: No dependencies.

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

FPT_TDC.1/Timestamping_Unit_Certificate Inter-TSF basic TSF data consistency

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [assignment: *fields of the imported time-stamping unit certificates*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [assignment: *the value of the timestamp public key contained in the imported timestamp certificate to verify it corresponds to the value of the non operational timestamp context public key generated during the timestamp context creation phase*] when interpreting the TSF data from another trusted IT product.

6.1.6 Trusted Path/Channels (FTP)

FTP_TRP.1/OCSP_And_Timestamping_Unit_Certificate Trusted path

Dependencies: No dependencies.

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

FTP_TRP.1.2 The TSF shall permit [selection: *local users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication*]

Application note: Local users referred to in these requirements are the Security Officers (S.OFFICER) of the TOE who import OCSP and time-stamping unit certificates into the TOE.

FTP_ITC.1/Trusted channel with the HSM Inter-TSF trusted channel

Dependencies: No dependencies.

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

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *Request for key pair generation, Request for list key pairs generated, Request for key pair deletion, Request for signature generation*].

FTP_ITC.1/Trusted channel with the Database Inter-TSF trusted channel

Dependencies: No dependencies.

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

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *All read operations between OCSP responder and the SQL Database over TLS, All read/write operations between Certstatus Feeder and the SQL Database over TLS*].

FTP_ITC.1/Trusted channel with the CA Gateway Inter-TSF trusted channel

Dependencies: No dependencies.

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

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *Request for certificates issued over TLS, Request for certificate revocation status changes over TLS*].

FTP_ITC.1/Trusted channel with the External Audit Server Inter-TSF trusted channel

Dependencies: No dependencies.

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

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *Send logs over TLS*].

6.1.7 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation

Dependencies: [FCS_CKM.2 Cryptographic key distribution or FCS_CKM.5 Cryptographic key derivation or FCS_COP.1 Cryptographic operation], FCS_CKM.3 Cryptographic key access, [FCS_RBG.1 Random bit generation (RBG) or FCS_RNG.1 Random number generation], FCS_CKM.6 Timing and event of cryptographic key destruction.

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *RSA PCKS#1 v.1.5, RSA-PSS; EC based DSA algorithm - Curve family NIST*] and specified cryptographic key sizes [assignment: *For RSA: 2048 bits, 3072 bits, 4096 bits; for ECDSA: ECC prime256v1 bits, prime384v1 bits and prime521v1 bits*] that meet the following: [assignment: *PKCS#1 RSA Cryptography Standard, FIPS 186-4 Digital Signature Standard (DSS), IETF RFC 3447*].

Application note: This requirement concerns the asymmetric key pairs used to create and verify the signature of OCSP responses generated by an OCSP unit and the signature of timestamping tokens generated by a timestamping unit. The key pairs shall be generated by the cryptographic module, whereas the key pair generation shall be invoked by the TOE.

FCS_CKM.3 Cryptographic Key Access

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation or FCS_CKM.5 Cryptographic key derivation].

FCS_CKM.3.1 The TSF shall perform [assignment: accesses specified in FCS_COP.1] in accordance with a specified cryptographic key access method [assignment: methods implemented by the CSP modules] that meets the following: [assignment: none].

FCS_CKM.6 Timing and event of cryptographic key destruction

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

FCS_CKM.6.1 The TSF shall destroy [assignment: *private keys contained in both operational and non operational OCSP and time-stamp service contexts*] when [selection: [assignment: when requested]].

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: active overwriting of the portion of memory containing the key] that meets the following: [assignment: none].

Application note: This requirement concerns private keys contained in both operational and non operational OCSP and time-stamp service contexts. This operation is performed by the cryptographic module on demand of the TOE.

FCS_COP.1 Cryptographic operation

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes or FCS_CKM.1 Cryptographic key generation, or FCS_CKM.5 Cryptographic key derivation], FCS_CKM.3 Cryptographic key access.

FCS_COP.1.1 The TSF shall perform [assignment: digital signature generation and verification] in accordance with a specified cryptographic algorithm [assignment: *RSA PCKS#1 v.1.5; RSA-PSS; EC based DSA algorithm - Curve family FIPS Publication 186-4*] and cryptographic key sizes [assignment: *For RSA: 2048, 3072 bits, 4096; For ECDSA: NIST P-256, NIST P-384, NIST P-521*] that meet the following: [*For RSA: PKCS#1 RSA Cryptography Standard, FIPS 186-4 Digital Signature Standard (DSS), IETF RFC 3447; For ECDSA: FIPS Publication 186-4*].

Application note: This requirement refers to digitally signing the OCSP responses and timestamp tokens generated by the TOE.

FCS_RNG.1 Random number generation

Dependencies: No dependencies.

FCS_RNG.1.1 The TSF shall provide a [selection: physical] random number generator that implements: [assignment: AIS 31 class PTG.2 according to [AIS31]:

(PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output;

(PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source;

(PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected;

(PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon;

(PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered continuously. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.].

FCS_RNG.1.2 The TSF shall provide [selection: octets of bits] that meet [assignment: AIS 31 class PTG.2 according to [AIS31]: (PTG.2.6) Test procedure A and none does not distinguish the internal random numbers from output sequences of an ideal RNG; (PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997].

Application note: This requirement refers to digitally signing the OCSP responses and timestamp tokens generated by the TOE.

FCS_TLSC_EXT.1 / TLS communications with the Database

Dependencies: No dependencies.

FCS_TLSC_EXT.1.1 The TSF shall implement [selection: *TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446)*] supporting the following ciphersuites: [selection:

TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF [selection: *does not provide*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid [selection: *without any administrator override mechanism*].

FCS_TLSC_EXT.1/TLS communications with the CA Gateway

Dependencies: No dependencies.

FCS_TLSC_EXT.1.1 The TSF shall implement [selection: *TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446)*] supporting the following ciphersuites: [selection: *TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF [selection: *does not provide*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid [selection: *without any administrator override mechanism*].

FCS_TLSC_EXT.1/TLS communications with the External Audit Server

Dependencies: No dependencies.

FCS_TLSC_EXT.1.1 The TSF shall implement [selection: *TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446)*] supporting the following ciphersuites: [selection: *TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,*

TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF [selection: *does not provide*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid [selection: *without any administrator override mechanism*].

FCS_TLSS_EXT.1/TLS communications with the Auditor

Dependencies: No dependencies.

FCS_TLSS_EXT.1.1 The TSF shall implement [selection: *TLS 1.2 (RFC 5246), TLS 1.3 (RFC 8446)*] supporting the following ciphersuites: [selection: *TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256*] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using [selection: *RSA with key size [selection: 2048, 3072, 4096] bits; ECDSA over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves*].

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using: [selection: *EC Diffie-Hellman key agreement over NIST curves [secp256r1, secp384r1, secp521r1], Curve25519 (X25519) as defined in RFC 7748] and no other curves;*]

6.1.8 Identification and Authentication (FIA)

FIA_UID.2 User identification before any action

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each ~~user~~ *Security Officer (S.OFFICER) and Auditor (S.AUDITOR)* to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.2 User authentication before any action

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each *Security Officer (S.OFFICER) and Auditor (S.AUDITOR)* to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.9 Security Audit (FAU)

FAU_GEN.1 Audit data generation

Dependencies: FPT_STM.1 Reliable time stamps

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 [selection: *not specified*] level of audit; and

c) [assignment:

- *TOE initialization,*
- *TOE start-up,*
- *Start of OCSP service operation,*
- *Stop of OCSP service operation,*
- *Generation of OB.OCSP_KEY_PUB and OB.OCSP_KEY_PRIV pairs*
- *Destruction of OB.OCSP_KEY_PUB and OB.OCSP_KEY_PRIV pairs*
- *OCSP response generation*
- *Start of TSU operation,*
- *Stop of TSU operation,*
- *Generation of OB.TST_KEY_PUB and OB.TST_KEY_PRIV pairs*
- *Destruction of OB.TST_KEY_PUB and OB.TST_KEY_PRIV pairs*

- *Time-stamp generation*
- *Users and roles management operations*
- *Successful and unsuccessful operations, including*
  - *Attempts of initiating a user session*
  - *Access to the security attributes of the OB.OCSP_CONTEXT.*
  - *Access to the security attributes of the OB.TST_CONTEXT.*
  - *Unsuccessful attempts to access the TOE resources.*
- *Value changes in OB.OCSP_CONTEXT*
- *Value changes in OB.TST_CONTEXT*
- *Desynchronization of the TOE*
- *Last successful synchronization check,*
- *Manual synchronization (date of synchronization operation and value of synchronization correction),].*

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [assignment: *Auditors (S.AUDITOR)*] with the capability to read [assignment: *list of audit information*] from the audit data.

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

FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to [assignment: *apply searching, sorting and ordering*] of audit data based on [assignment: *type of events, date of events*].

FAU_STG.2 Guarantees of audit data availability

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.2.2 The TSF shall be able to [selection: *prevent*] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.4 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [assignment: *overwrite the oldest stored audit records*] if the audit data storage exceeds [assignment: *80% of the threshold for total audit log storage capacity*].

6.2 Security Assurance Requirements

The development and the evaluation of the TOE shall be done in accordance with security assurance requirements corresponding to the Evaluation Assurance Level 4 augmented (EAL4+) with ALC_FLR.2 Flaw reporting procedures.

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)
	ALC_FLR.2 Flaw reporting procedures

Security Target evaluation (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	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)	AVA_VAN.3 Focused vulnerability analysis

Table 4. Security Assurance Requirements

6.3 Security Requirements Rationale

6.3.1 Security functional requirements rationale

6.3.1.1 SFR dependencies rationale

The following table displays the SFR dependencies:

SFR	Required Dependency	Dependency Satisfaction
User Data Protection		
FDP_ACC.1/ Context_Management_Policy	FDP_ACF.1	FDP_ACF.1/Context_Management_Policy
FDP_ACF.1/ Context_Management_Policy	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/Context_Management_Policy FMT_MSA.3/Context_Management_Policy
FDP_ITC.1/ Context_Management_Policy	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1/Context_Management_Policy FMT_MSA.3/Context_Management_Policy
FDP_ITC.2/ Context_Management_Policy	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	FDP_ACC.1/Context_Management_Policy FTP_TRP.1/ OCSP_And_Timestamping_Unit_Certificate FPT_TDC.1/OCSP_Unit_Certificate

		FPT_TDC.1/Timestamping_Unit_Certificate
FDP_ETC.1/ Non_Operational_Context_Public_Key	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1/Key_Management_Policy
FDP_ITC.2/ OCSP_And_Timestamp_unit_Certificate	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	FDP_IFC.1/Key_Management_Policy FTP_TRP.1/ OCSP_And_Timestamping_Unit_Certificate FPT_TDC.1/OCSP_Unit_Certificate FPT_TDC.1/Timestamping_Unit_Certificate
FDP_IFC.1/Key_Management_Policy	FDP_IFF.1	FDP_IFF.1/Key_Management_Policy
FDP_IFF.1/Key_Management_Policy	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Key_Management_Policy FMT_MSA.3/Context_Management_Policy
FDP_ACC.1/ OCSP_Response_Generation_Policy	FDP_ACF.1	FDP_ACF.1/ OCSP_Response_Generation_Policy
FDP_ACF.1/ OCSP_Response_Generation_Policy	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/ OCSP_Response_Generation_Policy FMT_MSA.3/ OCSP_Response_Generation_Policy
FDP_OCSP_EXT.1 / OCSP Response issuance	None	N/A
FDP_ACC.1/ Timestamp_Token_Generation_Policy	FDP_ACF.1	FDP_ACF.1/ Timestamp_Token_Generation_Policy
FDP_ACF.1/ Timestamp_Token_Generation_Policy	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1/ Timestamp_Token_Generation_Policy FMT_MSA.3/ Timestamp_Token_Generation_Policy
FDP_TST_EXT.1 / Time Stamp Tokens issuance	None	N/A
Security Management		
FMT_MSA.1/ Context_Management_Policy	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/Context_Management_Policy FMT_SMR.1 FMT_SMF.1/Context_Management_Policy
FMT_MSA.1/Multiple_Policies	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/Context_Management_Policy FDP_IFC.1/Key_Management_Policy FMT_SMR.1 FMT_SMF.1/Context_Management_Policy FMT_SMF.1/Temporary_Interruption

		FMT_SMF.1/Date_and_Time
FMT_MSA.3/ Context_Management_Policy	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Context_Management_Policy FMT_SMR.1
FMT_SMF.1/ Context_Management_Policy	None	N/A
FMT_MSA.1/Date_and_Time	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1/ Timestamp_Token_Generation_Policy FMT_SMR.1 FMT_SMF.1/Date_and_Time
FMT_MSA.3/Date_and_Time	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1/Date_and_Time FMT_SMR.1
FMT_SMF.1/ Date_and_Time	None	N/A
FMT_MTD.1/ Date_and_Time	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1/Date_and_Time
FMT_SMF.1/Temporary_Interruption	None	N/A
FMT_SMR.1	FIA_UID.1	FIA_UID.2
Protection of the TSF		
FPT_TDC.1/OCSP_Unit_Certificate	None	N/A
FPT_TDC.1/ Timestamping_Unit_Certificate	None	N/A
FPT_STM.1	None	N/A
Trusted Path/Channels		
FTP_TRP.1/ OCSP_And_Timestamping_Unit_Certificate	None	N/A
Cryptographic Support		
FCS_CKM.1	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1] FCS_CKM.3 [FCS_RBG.1 or FCS_RNG.1] FCS_CKM.6	FCS_CKM.2 FCS_CKM.3 FCS_RNG.1 FCS_CKM.6
FCS_CKM.3	[FDP_ITC.1 or FDP_ITC.2 or	FCS_CKM.1

	FCS_CKM.1 or FCS_CKM.5]	
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_RNG.1	None	N/A
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.3	FCS_CKM.1 FCS_CKM.3
Identification and Authentication		
FIA_UID.2	None	N/A
FIA_UAU.2	FIA_UID.1	FIA_UID.2
Security Audit		
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.2	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.2	FAU_STG.2

Table 5. SFR dependencies

6.3.1.2 SFR vs TOE security objectives rationale

The following table shows the correspondence between the security objectives applicable to the TOE and the defined security functional requirements.

	O.AUDIT	O.USER_AUTHENTICATION	O.RBAC	O.PUBLIC_KEY_MANAGEMENT	O.SYNCHRONISATION	O.AUDIT_PROTECTION	O.CRYPTO	O.OCSP_R	O.TXT
FDP_ACC.1/Context_Management_Policy			X						
FDP_ACF.1/Context_Management_Policy			X						
FMT_MSA.3/Context_Management_Policy			X	X					
FMT_MSA.1/Context_Management_Policy			X	X					
FMT_MSA.1/Multiple_Policies			X	X					
FMT_SMF.1/Context_Management_Policy				X					
FDP_ITC.1/Context_Management_Policy				X					
FDP_ITC.2/Context_Management_Policy				X					
FDP_ETC.1/Non_Operational_Context_Public_Key				X					
FDP_ITC.2/ OCSP_And_Timestamp_unit_Certificate				X					
FPT_TDC.1/OCSP_Unit_Certificate				X					
FPT_TDC.1/Timestamping_Unit_Certificate				X					
FTP_TRP.1/ OCSP_And_Timestamping_Unit_Certificate				X					
FDP_IFC.1/Key_Management_Policy				X					
FDP_IFF.1/Key_Management_Policy				X					
FCS_CKM.1							X		
FCS_CKM.6							X		

FCS_CKM.3							X		
FCS_RNG.1							X		
FMT_MSA.3/Date_and_Time					X				
FMT_MSA.1/Date_and_Time					X				
FMT_SMF.1/Date_and_Time					X				
FMT_MTD.1/Date_and_Time					X				
FDP_ITC.1/Date_and_Time					X				
FMT_SMF.1/Temporary_Interruption					X				
FDP_ACC.1/OCSP_Response_Generation_Policy			X						
FDP_ACF.1/OCSP_Response_Generation_Policy			X						
FDP_OCSP_EXT.1.1								X	
FDP_ACC.1/Timestamp_Token_Generation_Policy			X						
FDP_ACF.1/Timestamp_Token_Generation_Policy			X						
FDP_TST_EXT.1.1									X
FCS_COP.1							X		
FMT_SMR.1		X							
FIA_UID.2		X							
FIA_UAU.2		X							
FAU_GEN.1	X								
FAU_SAR.1	X								
FAU_SAR.3	X								
FPT_STM.1	X								
FAU_STG.4						X			
FAU_STG.2						X			
FCS_TLSC_EXT.1/TLS communications with the Database	X							X	
FCS_TLSC_EXT.1/TLS communications with the CA Gateway	X							X	

FCS_TLSC_EXT.1/TLS communications with the External Audit Server						X			
FCS_TLSS_EXT.1/TLS communications with the Auditor						X			
FTP_ITC.1/Trusted channel with the HSM				X					
FTP_ITC.1/Trusted channel with the Database	X							X	
FTP_ITC.1/Trusted channel with the CA Gateway	X							X	
FTP_ITC.1/Trusted channel with the External Audit Server						X			

Table 6 — Mapping between Security Objectives and Security Functional Requirements

Security functional requirements (SFR) coverage is met as each security objective is addressed by at least one SFR, and every SFR is mapped to at least one security objective.

Next, the rationale for each matching is provided:

O.AUDIT is covered by FAU_GEN.1, which ensures that event audit trails are generated by FPT_STM.1, which ensures that the date and time is reliable. This objective is also covered by FAU_SAR.1 and by FAU_SAR.3, ensuring the consultation of the audit logs. Moreover, this objective is also covered by FCS_TLSC_EXT.1/TLS communications with the Database, FCS_TLSC_EXT.1/TLS communications with the CA Gateway, FTP_ITC.1/Trusted channel with the Database and FTP_ITC.1/Trusted channel with the CA Gateway, ensuring the integrity of the communications with the Database and the CA Gateway component.

O.USER_AUTHENTICATION is covered by FIA_UID.2 and FIA_UAU.2, requiring identification and authentication of the different users and roles before any administrative or audit operation can take place.

Moreover, this objective is also covered by FMT_SMR.1 requiring the maintenance of the different roles by the TOE.

O.RBAC is covered by the context management policy :

- FDP_ACC.1/Context_Management_Policy,
- FDP_ACF.1/Context_Management_Policy,
- FMT_MSA.1/Context_Management_Policy
- FMT_MSA.1/Multiple_Policies
- FMT_MSA.3/Context_Management_Policy

In particular, this policy controls the operation for creating and modifying OCSP context and timestamping context. This Objective is also covered by the OCSP

response generation policy (FDP_ACC.1/OCSP_Response_Generation_Policy, FDP_ACF.1/OCSP_Response_Generation_Policy) and Time-Stamping token generation policy (FDP_ACC.1/Timestamp_Token_Generation_Policy, FDP_ACF.1/Timestamp_Token_Generation_Policy).

O.PUBLIC_KEY_MANAGEMENT is first covered by the context management policy:

- FMT_MSA.1/Context_Management_Policy
- FMT_MSA.1/Multiple_Policies
- FMT_MSA.3/Context_Management_Policy
- FMT_SMF.1/ Context_Management_Policy and

In particular, this policy controls the operation for creating, modifying, consulting and destroying the OCSP context. It is also covered by FDP_ITC.1/Context_Management_Policy and FDP_ITC.2/Context_Management_Policy which refers to the OCSP and time stamping context management policies regarding the import of information needed for context creation.

This objective is also covered by FDP_ETC.1/Non_Operational_Context_Public_Key and FDP_ITC.2/OCSP_And_Timestamp_unit_Certificate, referring to the key management policy regarding the export of the public key and the import of the corresponding certificate.

FPT_TDC.1/OCSP_Unit_Certificate ensures an adequate interpretation of particular certificates fields, particularly the value of the public key. Moreover, FTP_TRP.1/OCSP_And_Timestamping_Unit_Certificate ensures a trusted path with the Administrator when importing the OCSP unit certificate.

FPT_TDC.1/Timestamping_Unit_Certificate ensures an adequate interpretation of particular certificates fields, particularly the value of the public key. Moreover, FTP_TRP.1/OCSP_And_Timestamping_Unit_Certificate ensures a trusted path with the Administrator when importing the Timestamping unit certificate.

This objective is also covered by the Key Management (FDP_IFC.1/Key_Management_Policy and FDP_IFF.1/Key_Management_Policy).

This objective is also covered by the requirement FTP_ITC.1/Trusted channel with the HSM, ensuring integrity in the communications with the HSM.

O.SYNCHRONISATION is covered by FMT_MTD.1/Date_and_Time, ensuring that the internal date and time is initially synchronized by an administrator during the time stamping initialization process. It is also ensured by FMT_SMF.1/Date_and_Time, requiring a following of the synchronization with UTC according to a specific precision level. This objective is also covered by

FDP_ITC.1/Date_and_Time, referring to the timestamping generation policy based on the synchronization state. FMT_MSA.1/Date and Time and FMT_MSA.3/Date_and_Time are also covering this objective due to the limitation of modifying the synchronization state to an authenticated Security Officer. FPT_STM.1 ensures that the date associated to each event is reliable.

This objective is covered FMT_SMF.1/Temporary_Interruption, ensuring the monitoring of the synchronization state of the timestamping service and ensures the stop of the service in case of lose of synchronization.

O.AUDIT_PROTECTION is covered by FAU_STG.2 and FAU_STG, than ensure protection of the audit logs in integrity and ensure the availability of the logs. In addition, FCS_TLSS_EXT.1/TLS communications with the Auditor ensures integrity for the communications between the TOE and the Auditor, and FTP_ITC.1/Trusted channel with the External Audit Server and FCS_TLSC_EXT.1/TLS communications with the External Audit Server, ensuring a trusted channel with the External Audit Server.

O.CRYPTO is covered by all SFRs related to cryptographic key management and cryptographic operations:

- FCS_COP.1
- FCS_CKM.6
- FCS_CKM.3
- FCS_RNG.1
- FCS_CKM.1

O.OCSP_R is covered by FDP_OCSP_EXT.1.1, ensuring that the OCSP response issued by the TOE contains security values in accordance with IETF RFC 6960. Moreover, this objective is also covered by FCS_TLSC_EXT.1/TLS communications with the Database, FCS_TLSC_EXT.1/TLS communications with the CA Gateway, FTP_ITC.1/Trusted channel with the Database and FTP_ITC.1/Trusted channel with the CA Gateway, ensuring the integrity of the communications with the Database and the CA Gateway component.

O.TST is covered by FDP_TST_EXT.1.1, ensuring that the Time Stamp Token issued by the TOE contains security values in accordance with IETF RFC 3161.

6.3.2 Security assurance requirements rationale

6.3.2.1 Assurance level table

Assurance level	Required Dependency	Element Satisfying the Dependency

ADV_ARC.1	(ADV_FSP .1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_TDS.3	(ADV_FSP .4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No dependency	
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ALC_CMC.3	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.3, ALC_DVS.1, ALC_LCD.1
ALC_CMS.3	No dependency	
ALC_DEL.1	No dependency	
ALC_DVS.1	No dependency	
ALC_FLR.2	No dependency	
ALC_LCD.1	No dependency	
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependency	
ASE_INT.1	No dependency	
ASE_OBJ.2	(ASE_SPD.1)	(ASE_SPD.1)
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependency	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1) and (ADV_FSP.2) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1

Table 7. Assurance level table

6.3.2.2 EAL rationale

The Security Assurance Requirements (SAR) for this Security Target have been selected according to the Evaluation Assurance Level 4 augmented (EAL4+) ALC_FLR.2.

EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4+ ALC_FLR.2 is appropriate for commercial products that can be applied to moderate to medium-high security functions, and resist to enhanced-basic attack potential. The TOE described in this Security Target is such a product.

7 TOE Summary specification

7.1 User Data Protection (FDP)

FDP_ACC.1/Context_Management_Policy Subset access control

When the TOE is initialized, an OS user called `sysadmin` is created and configured with the necessary permissions to manage the OB.OCSP_CONTEXT and the OB.TST_CONTEXT. The `sysadmin` OS user is the one that the S.OFFICER role uses for performing the needed operations on the *OB.OCSP_CONTEXT* and the OB.TST_CONTEXT.

The *S.OFFICER* role uses the `sysadmin` OS user credentials to connect to the TOE. This connection can be done either using the Secure Shell Protocol (SSH) or using the physical terminal of the machine where the TOE is located.

When the TOE is initialized, an internal component named Auth Service is deployed. This component acts as an *Identity Provider* (IdP).

A key pair (consisting of a public and private key) is generated during the Auth Service deployment process. The Auth Service key pair is different in each TOE installation. The private key contents are stored in a Kubernetes Secret, which is created in the Auth Service specific Kubernetes namespace. The public key contents are stored in a Kubernetes ConfigMap, which is created in the Auth Service specific Kubernetes namespace.

The Kubernetes Secret containing the private key and the Kubernetes ConfigMap containing the public key are injected into the Auth Service Kubernetes Pod, and therefore consumed as environment variables. The Auth Service configuration file, which references the environment variables containing the private key and public key, is stored as a Kubernetes Secret, which is created in the Auth Service specific Kubernetes namespace. The Kubernetes Secret containing the Auth Service configuration file Is mounted into the Auth Service Kubernetes Pod as a volume in the Auth Service container. The Auth Service container in the Kubernetes Pod loads the configuration file when initialized. The values of the private key and public key are never stored clear on the disk.

Kubernetes Secrets in the TOE are encrypted at rest. When Kubernetes is initialized, it generates an AES-CBC key. With this key, it generates a Kubernetes `EncryptionConfiguration` file. This file is passed to the kube-apiserver component with the `encryption-provider-config` configuration field to enable the data encryption at rest. The Kubernetes `EncryptionConfiguration` file is stored in the OS, protected with `root` OS permissions. The Kubernetes `EncryptionConfiguration` file is different in each TOE installation.

When the Auth Service component is initialized, three Auth Service roles are created, with their assigned scope permissions:

- `RootRole`:
  - `user,manage`: Manage all the users in the system.
  - `role,manage`: Manage all the roles in the system.
  - `idp,manage`: Manage all the Auth Service authorization configuration.
- `CliRole`:
  - `solution,manage:all`: Manage all the solutions in the system.
  - `user,manage`: Manage all the users in the system.
  - `role,manage`: Manage all the roles in the system.
- `AdminRole`:
  - `solution,manage:all`: Manage all the solutions in the system.
  - `user,manage`: Manage all the users in the system.
  - `role,manage`: Manage all the roles in the system.
  - `idp,manage`: Manage all the Auth Service authorization configuration.

When the Auth Service component is initialized, three Auth Service users are created, with their assigned Auth Service roles:

- `root`:
  - Internal user used to create the solution users and roles on the Auth Service.
  - Configured with the `RootRole` role.
- `cli`:
  - Internal user used to authenticate the CLI with the Solution Manager APIs.
  - Configured with the `CliRole` role.
- `admin`:
  - Default Management Console user used to manage the solutions from the Management Console.
  - Configured with the `AdminRole` role.

For the `root` and `cli` Auth Service user, a password credential is generated during the Auth Service deployment. Each password credentials are stored in its own Kubernetes Secret, which is created in the Auth Service specific Kubernetes namespace. The password credentials are different in each TOE installation.

The Kubernetes Secrets containing the password credentials of the `root` and `cli` Auth Service users are injected into the Auth Service Kubernetes Pod, and therefore consumed as environment variables. The Auth Service configuration file also references the environment variables containing the `root` and `cli` Auth Service user passwords. The values of the `root` and `cli` Auth Service user passwords are never stored clear on the disk.

For performing the OP.OCSP_CONTEXT_CREATION, OP.OCSP_CONTEXT_MODIFICATION, OP.OCSP_CONTEXT_DESTRUCTION, OP.OCSP_CONTEXT_CONSULTATION operations on the OB.OCSP_CONTEXT or the OP.TST_CONTEXT_CREATION, OP.TST_CONTEXT_MODIFICATION, OP.TST_CONTEXT_DESTRUCTION, OP.TST_CONTEXT_CONSULTATION operations on the OB.TST_CONTEXT, the S.OFFICER uses the `sysadmin` OS user to execute the `clusterctl` CLI tool. The S.OFFICER, using the `sysadmin` OS user, needs to elevate OS privileges (using `sudo`) to execute the `clusterctl` CLI tool.

The `clusterctl` CLI tool uses the `kubectl` CLI tool to access the Kubernetes API. To authenticate with the Kubernetes API, the `kubectl` CLI tool is configured with a `kubeconfig` file, which contains the necessary credentials to obtain full access to the Kubernetes API. The `kubeconfig` file is protected with `root` OS permissions.

The `clusterctl` CLI tool uses the `kubectl` CLI tool to obtain the password value of the Auth Service `cli` user, which is stored in a Kubernetes Secret in the Auth Service specific Kubernetes namespace. The `clusterctl` CLI tool accesses the Auth Service Login API and authenticates using the `cli` username and the obtained password. Once the request is successful, the Auth Service Login API returns a *JSON Web Token* (JWT), which is configured with the scope permissions of the Auth Service `CliRole`. The `clusterctl` CLI tool uses the obtained JWT to authenticate with the Solution Manager APIs.

When the TOE is initialized, an internal component named Solution Manager is deployed. This component is the responsible of managing the OB.OCSP_CONTEXT and the OB.TST_CONTEXT.

The Kubernetes Secrets containing the Auth Service public key and the password credentials of the `root` Auth Service user are injected into the Solution Manager Kubernetes Pod, and therefore consumed as environment variables. The Solution Manager container in the Kubernetes Pod loads the environment variables contents when initialized.

The Solution Manager APIs require to specify an Authorization Token in the request. The Solution Manager uses the Auth Service public key to validate the JWT specified in the request, validating the JWT signature and comparing the presented scopes in the JWT with the defined scopes of each Solution Manager API endpoint.

For performing the OP.OCSP_CONTEXT_CREATION, OP.OCSP_CONTEXT_MODIFICATION, OP.OCSP_CONTEXT_DESTRUCTION, and OP.OCSP_CONTEXT_CONSULTATION operations on the *OB.OCSP_CONTEXT*, the *S.OFFICER* uses the `sysadmin` OS user to execute the `evactl` CLI tool. The *S.OFFICER*, using the `sysadmin` OS user, needs to elevate OS privileges (using `sudo`) to execute the `evactl` CLI tool.

The `evactl` CLI tool uses the `kubectl` CLI tool to access the Entrust PKI Hub configuration files and export the Entrust PKI Hub secrets related to the OCSP service. The `evactl` CLI tool uses the `clusterctl` CLI tool to import the Entrust PKI Hub secrets related to the OCSP service.

The *S.OFFICER* uses the `sysadmin` OS user to execute the `clusterctl` CLI tool and the `evactl` CLI tool to perform the OP.OCSP_CONTEXT_CREATION, OP.OCSP_CONTEXT_MODIFICATION, OP.OCSP_CONTEXT_DESTRUCTION, and OP.OCSP_CONTEXT_CONSULTATION operations on the OB.OCSP_CONTEXT.

For performing the OP.TST_CONTEXT_CREATION, OP.TST_CONTEXT_MODIFICATION, OP.TST_CONTEXT_DESTRUCTION, and OP.TST_CONTEXT_CONSULTATION operations on the *OB.TST_CONTEXT*, the *S.OFFICER* uses the `sysadmin` OS user to execute the `tsactl` CLI tool. The *S.OFFICER*, using the `sysadmin` OS user, needs to elevate OS privileges (using `sudo`) to execute the `tsactl` CLI tool.

The `tsactl` CLI tool uses the `kubectl` CLI tool to access the Entrust PKI Hub configuration files and export the Entrust PKI Hub secrets related to the time-stamp service. The `tsactl` CLI tool uses the `clusterctl` CLI tool to import the Entrust PKI Hub secrets related to the time-stamp service.

FDP_ACF.1/Context_Management_Policy Security attribute based access control

As explained in FDP_ACC.1, when the TOE is initialized, an OS user called `sysadmin` is created and configured with the necessary permissions to manage the OB.OCSP_CONTEXT, OB.TST_CONTEXT and the SFP-relevant security attributes. The `sysadmin` OS user is the one that the S.OFFICER role uses for performing the needed operations on the OB.OCSP_CONTEXT and the OB.TST_CONTEXT.

The S.OFFICER role uses the `sysadmin` OS user credentials to connect to the TOE. This connection can be done by using the *Secure Shell Protocol* (SSH), the *Secure File Transfer Protocol* (SFTP) or using the physical terminal of the machine where the TOE is located.

To perform the OP.OCSP_CONTEXT_CREATION, OP.OCSP_CONTEXT_MODIFICATION, OP.OCSP_CONTEXT_DESTRUCTION,

OP.TST_CONTEXT_CREATION, OP.TST_CONTEXT_MODIFICATION, and OP.TST_CONTEXT_DESTRUCTION, the S.OFFICER will need to use the `sysadmin` OS credentials twice. The S.OFFICER imports the OB.OCSP_CONTEXT and the OB.TST_CONTEXT inside the TOE OS filesystem by connecting to it by SFTP. At that point the imported contexts are not usable yet by the TOE. To import the contexts inside the TOE, now the S.OFFICER authenticates using either SSH or the physical terminal with the `sysadmin` credentials into the TOE OS and then makes use of the `clusterctl` command to import the contexts (see FDP_ACC.1). There are no other OS credentials that could make use of the SFTP, SSH or physical terminal.

As explained in FDP_ACC.1, there are three internal components that takes part on the contexts import: the Kubernetes API, the Auth Service and the Solution Manager. All those components are only accessible from other TOE components (i.e. their interfaces are not exposed outside the TOE). In particular, the credential to use the Kubernetes API is protected by root. This credential is used from either, the `evactl`, `tsactl` and `clusterctl` commands. From the `evactl` and `tsactl`, it is used to retrieve secrets directly from Kubernetes. From the `clusterctl`, it is used to retrieve the CLI credentials to login to the Auth Service. One logged in, a JWT could be obtained from the Auth Service to access the Solution Manager component and finally manage the OB.OCSP_CONTEXT and OB.TST_CONTEXT into the TOE. Note that `evactl` and `tsactl` also uses `clusterctl` to do some of the operations offered by the Solution Manager.

To perform the OP.OCSP_CONTEXT_CONSULTATION the S.OFFICER has to access the TOE OS by either SSH or the physical terminal using the `sysadmin` credentials. After this, they can make use of either the `clusterctl` or `evactl` commands to obtain the OB.OCSP_CONTEXT.

To perform the OP.TIMESATMP_CONTEXT_CONSULTATION the S.OFFICER has to access the TOE OS by either SSH or the physical terminal using the `sysadmin` credentials. After this, can make use of either the `clusterctl` or `tsactl` commands to obtain the OB.TST_CONTEXT.

The S.AUDITOR has no credentials that allows any of the previous operations.

FDP_ITC.2/Context_Management_Policy Import of user data with security attributes

As explained in FDP_ACF.1, only the S.OFFICER can import the OB.OCSP_CONTEXT into the TOE OS via Secure File Transfer Protocol (SFTP) and import into the TOE via the `clusterctl` or `evactl` commands.

As explained in FDP_ACF.1, only the S.OFFICER can import the OB.TST_CONTEXT into the TOE OS via Secure File Transfer Protocol (SFTP) and import into the TOE via the `clusterctl` or `tsactl` commands.

S.AUDITOR and the unauthenticated users don't have the required OS privileges to interact with OB.OCSP_CONTEXT and OB.TST_CONTEXT.

FDP_ETC.1/Non_Operational_Context_Public_Key Export of user data without security attributes

Only the S.OFFICER can export the OB.OCSP_PUB_KEY by means of the `evactl create-key` or `create-csr` commands. The value of the public key is exported as part of a CSR that allows the user to easily process that CSR in order to issue the corresponding OCSP certificate.

Only the S.OFFICER can export the OB.TST_PUB_KEY by means of the `tsactl create-key` or `create-csr` commands. The value of the public key is exported as part of a CSR that allows the user to easily process that CSR in order to issue the corresponding time-stamp certificate

FDP_ITC.2/OCSP_And_Timestamp_unit_Certificate Import of user data with security attributes

As explained in FDP_ACC.1, when the TOE is initialized, an OS user called `sysadmin` is created and configured with the necessary permissions to manage the OB.OCSP_CONTEXT, the OB.TST_CONTEXT and the SFP-relevant security attributes. The `sysadmin` OS user is the one that the *S.OFFICER* role uses to perform the import of the OCSP and time-stamping services certificates.

The S.OFFICER role uses the `sysadmin` OS user credentials to connect to the TOE to import the OCSP and time-stamping services certificates . First the S.OFFICER connects to the TOE OS with the `sysadmin` credentials through *Secure File Transfer Protocol* (SFTP). Once authenticated, the S.OFFICER can import the OCSP and time-stamping services certificates inside the TOE OS.

After that, the S.OFFICER authenticates into the TOE OS either by *Secure Shell Protocol* (SSH) or the physical terminal using the mentioned credentials. Once authenticated, the S.OFFICER uses the clusterctl solution config import to import the OCSP service certificate and the time-stamping certificate.

FDP_IFC.1/Key_Management_Policy Subset information flow control

The only role authorized to import or export user data outside of the TOE is the S.OFFICER.

To import user data, it must authenticate into the TOE's OS using the `sysadmin` credentials that were created as part of the TOE initialization. First, the S.OFFICER will have to authenticate by SFTP using the `sysadmin` credentials. Once authenticated, the S.OFFICER can import the user data into the TOE's OS. Then, using the same credentials, the S.OFFICER has to authenticate into the TOE's OS by either SSH or the physical terminal. Then, by using the `evactl`, `tsactl` and `clusterctl` commands, the S.OFFICER will be able to import the user data from the TOE's OS into the TOE.

To export user data, it must authenticate into the TOE's OS using the `sysadmin` credentials that were created as part of the TOE initialization. First, the S.OFFICER will have to authenticate either by SSH or by the physical terminal using the `sysadmin` credentials. Then, by using the `evactl`, `tsactl` and `clusterctl` commands, the S.OFFICER will be able to export the user data into the TOE's OS. Once exported, the S.OFFICER will have to authenticate using SFTP to export the data outside of the TOE's OS.

The communication channel to import/export user data from the TOE's OS is SFTP. Once inside the TOE's OS, the `clusterctl` command will use a JWT token issued to its internal credentials by the Auth Service component to access the Solution Manager component and import/export the data into/from the TOE.

FDP_IFF.1/Key_Management_Policy Simple security attributes

The SFPs identified in the assignments of the requirements affect the following user data:

- R.OCSP_KEY_PAIR_PRIV: The OCSP private key is stored in the cryptographic module and never leaves the cryptographic module, so its integrity and confidentiality is preserved at all times.
- R.OCSP_KEY_PAIR_PUB: The public key is tied to the R.OCSP_KEY_PAIR_PRIV and can only be exported (as a CSR) by the S.OFFICER. The cryptographic properties of the key pair ensure that only a OCSP service certificate that can be validated using the R.OCSP_KEY_PAIR_PRIV can be imported.
- R.TST_KEY_PAIR_PRIV: The time-stamping private key is stored in the cryptographic module and never leaves the cryptographic module, so its integrity and confidentiality is preserved at all times.

- R.TST_KEY_PAIR_PUB: The public key is tied to the R.TST_KEY_PAIR_PRIV and can only be exported (as a CSR) by the S.OFFICER. The cryptographic properties of the key pair ensure that only a TSU certificate that can be validated using the R.TST_KEY_PAIR_PRIV can be imported.

FDP_ITC.1/Date_and_Time Import of user data without security attributes

The user data R.DATA_AND_TIME is set during the TSU initialization process and kept in sync with the reference NTP server while the TSU is operational. Only the S.OFFICER can modify the synchronization state of the TSU.

The Timestamping Generation Policy ensures that R.TST_TOKENs can only be generated when the R.DATA_AND_TIME is kept in synchronization state within the limits specified by the synchronization precision limit.

FDP_ACC.1/OCSP_Response_Generation_Policy Subset access control

Only the S.OFFICER can affect the OCSP response generation process by modifying the R.OCSP_CONTEXT elements that affect the generation of OCSP responses (R.OCSP_RESPONSE) like the OCSP policy, the key pair to be used or the certificate information source.

FDP_ACF.1/OCSP_Response_Generation_Policy Security attribute based access control

All the security attributes that affect the OCSP Response Generation Policy (AT.OPERATIONAL_OCSP_CONTEXT_COMPLETE,
AT.OCSP_CONTEXT_OPERATIONAL,
AT.OPERATIONAL_OCSP_CONTEXT_KEY_PAIR_CREATED, etc.) can only be modified by an authenticated S.OFFICER.

FDP_ACC.1/Timestamp_Token_Generation_Policy Subset access control

Only the S.OFFICER can affect the token generation process by either modifying the `chrony` configuration or by modifying the R.TST_CONTEXT elements that affect the generation of timestamp tokens (R.TST_TOKEN) like the default time-stamping policy, the key pair to be used or the allowed time precision limits (accuracy).

FDP_ACF.1/Timestamp_Token_Generation_Policy Security attribute based access control

All the security attributes that affect the Token Generation Policy (AT.OPERATIONAL_TST_CONTEXT_COMPLETE,
AT.TST_CONTEXT_OPERATIONAL,
AT.OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED,
AT.MONOTONIC_TIMESTAMP_TOKEN_TIME, etc.) can only be modified by an authenticated S.OFFICER.

FDP_OCSP_EXT.1 /OCSP Responses issuance

The OCSP service is compliant with IETF RFC 6960 so the received OCSP requests (OB.OCSP_REQUEST) are processed as described in *7.8.3 OCSP Response Generation Policy* to generate a proper OCSP response (OB.OCSP_RESPONSE).

FDP_TST_EXT.1 /Time Stamp Tokens issuance

The TSU is compliant with IETF RFC 3161 so the received timestamp requests (OB.TST_REQUEST) are processed as described in *7.8.4 Timestamp Token Generation Policy* to generate a proper time-stamping error response or a time-stamping signed token (OB.TST_TOKEN).

7.2 Security Management (FMT)

FMT_MSA.1/Context_Management_Policy Management of security attributes; FMT_MSA.1/Multiple_Policies Management of security attributes; FMT_MSA.3/Context_Management_Policy Static attribute initialization; FMT_SMF.1/Context_Management_Policy Specification of Management Functions

As explained in FDP_ACF.1, the S.OFFICER (by using the `sysadmin` credentials) is the only role allowed to change the OB.OCSP_CONTEXT (OP.OCSP_CONTEXT_CREATION, OP.OCSP_CONTEXT_DESTRUCTION, OP.OCSP_CONTEXT_MODIFICATION and OP.OCSP_UNIT_CERTIFICATE_IMPORT) and the OB.TST_CONTEXT (OP.TST_CONTEXT_CREATION, OP.TST_CONTEXT_DESTRUCTION, OP.TST_CONTEXT_MODIFICATION, OP.TST_UNIT_CERTIFICATE_IMPORT and OP.INIT_DATE_AND_TIME).

The S.AUDITOR and the unauthenticated users don't have access to any credential that allows manipulating either the OB.OCSP_CONTEXT or OB.TST_CONTEXT.

Any OCSP service will not start until the OB.OCSP_CONTEXT is valid to operate. During the initialization, before the AT.OCSP_CONTEXT_OPERATIONAL_COMPLETE is set by the S.OFFICER, the OCSP service can't start.

Any TSU will not start until the OB.TST_CONTEXT is valid to operate. During the initialization, before the AT.TST_CONTEXT_OPERATIONAL_COMPLETE is set by the S.OFFICER, the TSU can't start.

If the TSU environment is configured following the indications given in this ST, the AT.MONOTONIC_TIMESTAMP_TOKEN_TIME attribute will always be "True".

FMT_MSA.1/Date_and_Time Management of security attributes; FMT_MSA.3/Date_and_Time Static attribute initialization

The TOE relies on the system clock of the host for a reliable time stamp. The system clock can only be modified by a user that has `root` OS privileges. In order to synchronize the system clock with external NTP servers, the TOE includes `chrony` (see chrony – Introduction (chrony-project.org)), an implementation of the Network Time Protocol (NTP). Only the S.OFFICER, using the `sysadmin` OS user and elevating their OS privileges (using `sudo`) have those `root` OS privileges.

During the TOE installation, `chrony` is automatically configured to use the NTP server provided by DHCP. TSU cannot become operational until it can access the `chrony` service and the `chrony` service has properly synchronized its time with the external NTP server.

During the TOE initialization, the Security Officer must configure `chrony` to allow the TSUs to access `chrony` service and, optionally, to replace the default NTP servers configured if required.

FMT_SMF.1/Date_and_Time Specification of Management Functions

As explained in FMT_MSA.1 and FMT_MSA.3, the TOE includes `chrony` component that allows to synchronize the system clock with external NTP servers.

`chrony` allows to:

- Automatically synchronize the system clock with external NTP servers that have been configured. `chrony` daemon running in background computes the rate at which the system clock gains or loses time, and compensates the system clock at that same rate.

- Manually force the synchronization of the system clock with external NTP servers.
- Obtain statistics that report how far off the system clock is from the reference NTP server. This statistics can be compared with the accuracy defined in the operational context to define the value of the security attribute AT.DATE_AND_TIME_SYNCHRONIZED.

FMT_MTD.1/Date_and_Time Management of TSF data

As explained in FMT_MSA.1 and FMT_MSA.3, the TOE only allows the Security Officer, using the `sysadmin` OS user to modify the system clock and configure `chrony`.

FMT_SMF.1/Temporary_Interruption Specification of Management Functions

As explained in FMT_SMF.1/Date_and_Time Specification of Management Functions, `chrony` service allows the TSU to obtain statistics that report how far off the system clock is from the reference NTP server.

Entrust PKI Hub will interrupt the time-stamping service (stopping the time-stamp issuance) if the time difference between the system clock and the reference NTP is greater than the accuracy defined in the used operational context.

FMT_SMR.1 Security roles

The S.OFFICER role uses the `sysadmin` OS user to perform the majority of the operations in the TOE. The `sysadmin` OS user is able to elevate OS privileges using `sudo`.

The `sysadmin` OS user could be potentially deleted by the S.OFFICER role, by escalating OS privileges to the `root` OS user using `sudo`. However, as the `root` OS user has more privileges than the `sysadmin` OS user, and the `sysadmin` OS user can escalate OS privileges, the S.OFFICER role can perform the same operations in the TOE with the `sysadmin` OS user and with the `sysadmin` OS user.

The S.OFFICER role could potentially create new OS users, by escalating privileges to the `root` OS user with the `sysadmin` OS user. However, these new OS users will have less or equal privileges than the `sysadmin` OS user, and less privileges than the `root` OS user.

So, the TSF is able to maintain the S.OFFICER role.

The S.AUDITOR role uses the `admin` user to access the Grafana internal component, which is deployed when the TOE is initialized. Grafana is an observability and data visualization platform that allows to query, visualize, and explore logs and events.

The logs and events are stored in the Grafana Loki database internal component, which is deployed when the TOE is initialized. Grafana is configured with the Loki database as a data source, which enables to query, visualize, and explore the stored logs and events from the Grafana Graphical User Interface (GUI).

Grafana is configured with basic username and password authentication. A default user called `admin` is created during the Grafana deployment. The Entrust PKI Hub 1.0.0 documentation contains the default credentials (username and password) of the `admin` Grafana user.

Once the `admin` Grafana user is authenticated in the Grafana GUI, it can perform the following operations:

- Configuration
  - Edit the `admin` user preferences.
  - Change the `admin` user password.
- Server administration
  - Edit the `admin` user settings.
  - View the system settings.
  - View the statistics.
- Dashboards and Exploration
  - View the metrics, logs, and events in the dashboards

As the Grafana `admin` user is an administrator user, it has permission to perform almost any operation from the Grafana GUI (except modifying or deleting the Grafana system settings). Any operation of the described above can modify the scope of the S.AUDITOR or reduce the `admin` user capabilities.

7.3 Protection of the TSF (FPT)

FPT_TDC.1/OCSP_Unit_Certificate Inter-TSF basic TSF data consistency

The OCSP service certificate can be used by any interested party to validate the signature included in any OB.OCSP_RESPONSE generated by the OCSP service. This means that the OCSP service certificate is expected to be made public and shared with any users or auditors of the TOE to validate the TSF data consistency.

FPT_TDC.1/Timestamping_Unit_Certificate Inter-TSF basic TSF data consistency

The TSU Certificate can be used by any interested party to validate the signature included in any OB.TST_TOKEN generated by the TSU. This means that the TSU certificate is expected to be made public and shared with any users or auditors of the TOE to validate the TSF data consistency.

FPT_STM.1 Reliable time stamps

The TOE environment uses a NTP client that is synchronized with a NTP server in order to issue a reliable time source. The reliable time stamps are used in the events logs generated by the TOE.

7.4 Trusted Path/Channels (FTP)

FTP_TRP.1/OCSP_And_Timestamping_Unit_Certificate Trusted path

As explained in FDP_ITC.1, the S.OFFICER is the only authorized to import OCSP and time-stamping unit certificates into the TOE.

To import that certificate, the S.OFFICER must used Secure File Transfer Protocol (SFTP) to import the certificates in the OS filesystem. SFTP encrypts both the authentication process and the data transfer process, ensuring a double layer of security. The certificate files imported can be only read or modified it by the `sysadmin` user, as it is protected by the OS permissions.

As explained in FMT_MSA.1 and FMT_ACF.1, the S.OFFICER that is allowed to use `evactl` and `tsactl` via using the Secure Shell Protocol (SSH) or using the physical terminal of the machine where the TOE is located.

FTP_ITC.1/Trusted channel with the Database

The CertStatus feeder service receives from the CRL Shim and the CA Gateway Shim certificate status information and stores that information in the database. The CertStatus feeder acts as a client of the database, opening a secure TLS channel (TLS v1.2/1.3, server only authentication) to guarantee privacy (confidentiality), integrity and database authenticity. All read/write operations between Certstatus feeder and the database are over that TLS channel.

The CertStatus feeder verifies the database TLS server certificate using the CA certificate specified in the OB.OCSP_CONTEXT. It also checks that the database TLS certificate is not expired, and IP/hostname of the database corresponds to the specified in the database TLS server certificate.

FTP_ITC.1/Trusted channel with the CA Gateway

The CA Gateway Shim obtains from external CA Gateway certificate status information and send it to the CertStatus feeder. The CA Gateway Shim acts as a client of the CA Gateway, opening a secure TLS channel (TLS v1.2/1.3, mutual TLS authentication) to guarantee privacy (confidentiality), integrity and CA Gateway authenticity. All operations between CA Gateway Shim and the CA Gateway are over that TLS channel.

The CA Gateway Shim verifies the CA Gateway TLS server certificate using the CA certificate specified in the OB.OCSP_CONTEXT. It also checks that the database TLS certificate is not expired, and IP/hostname of the CA Gateway corresponds to the specified in the CA Gateway TLS server certificate.

FTP_ITC.1/Trusted channel with the External Audit Server

The TOE can forward the auditing logs to an external Security Information and Event Management (SIEM). The TOE acts as a client of the SIEM, opening a secure TLS channel (TLS v1.2/1.3, server only authentication) to guarantee privacy (confidentiality), integrity and SIEM authenticity. All operations between TOE and the SIEM are over that TLS channel.

The TOE verifies the database TLS server certificate using the CA certificate specified in the OB.TLS_CONTEXT. It also checks that the SIEM TLS certificate is not expired, and IP/hostname of the database corresponds to the specified in the SIEM TLS server certificate.

7.5 Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic key generation; FCS_CKM.6 Timing and event of cryptographic key destruction; FCS_RNG.1 Random number generation

OCSP key pair generation and destruction is done by means of the `evactl` CLI tool using the `create-key` and `delete-key` commands respectively. Both operations just trigger the corresponding operations on the HSM which is the one that really executes them. This ensures that the R.OCSP_KEY_PAIR_PRIV is always generated with all the security properties and protections provided by the HSM. OCSP service only stores locally a reference (handle) to that private key which really resides within the HSM.

A final step in the kay pair generation process is the generation and signing of a Certificate Signing Request (CSR) that can be used to generate the certificate corresponding to the OCSP service public key.

TSU Key pair generation and destruction is done by means of the `tsactl` CLI tool using the `create-key` and `delete-key` commands respectively. Both operations just trigger the corresponding operations on the HSM which is the one that really executes them. This ensures that the R.TST_KEY_PAIR_PRIV is always generated with all the security properties and protections provided by the HSM. TSU only stores locally a reference (handler) to that private key which really resides within the HSM.

A final step in the kay pair generation process is the generation and signing of a Certificate Signing Request (CSR) that can be used to generate the certificate corresponding to the TSU public key.

Application Note

The TOE uses a cryptographic module certified in conformance with [EN 419 221-5] for cryptographic operations.

FCS_COP.1 Cryptographic operation; FCS_CKM.3 Cryptographic key access

The OCSP service performs a signing operation (OP.OCSP_RESPONSE_SIGNATURE) as part of the generation of OCSP responses. The algorithm used for these signatures depends on the algorithm that was chosen for the OCSP service key pair generation.

The TSU performs a signing operation (OP.TST_TOKEN_SIGNATURE) as part of the generation of timestamp tokens. The algorithm used for these signatures depends on the algorithm that was chosen for the TSU key pair generation.

The generation of those signatures follows the Digital Signature Standard [FIPS Pub 186].

FCS_TLSC_EXT.1 / TLS communications with the Database

As explained in FTP_ITC.1/Trusted channel with the Database, the CertStatus feeder opens a secure TLS channel (TLS v1.2/1.3, server only authentication) with the database to guarantee privacy (confidentiality), integrity and database authenticity.

FCS_TLSC_EXT.1/TLS communications with the CA Gateway

As explained in FTP_ITC.1/Trusted channel with the CA Gateway, the TOE opens a secure TLS channel (TLS v1.2/1.3, server only authentication) with the CA

Gateway component to guarantee privacy (confidentiality), integrity and database authenticity.

FCS_TLSC_EXT.1/TLS communications with the External Audit Server

As explained in FTP_ITC.1/Trusted channel with the External Audit Server, the TOE opens a secure TLS channel (TLS v1.2/1.3, server only authentication) with the SIEM to guarantee privacy (confidentiality), integrity and database authenticity.

FCS_TLSS_EXT.1/TLS communications with the Auditor

The TOE offers the Auditor GUI (Grafana) service through an HTTPS (HTTP over TLS) interface. The Auditor GUI acts as a TLS server, encrypting the traffic with the Auditor using a secure TLS channel (TLS v1.2/1.3, server only authentication).

The Auditor GUI encrypts the traffic using the TLS certificate specified in the OB.TLS_CONTEXT.

7.6 Identification and Authentication (FIA)

FIA_UID.2 User identification before any action; FIA_UAU.2 User authentication before any action

As explained in FDP_ACC.1 and FMT_SMR.1, during the TOE initialization, the default credentials (username/password) for S.OFFICER and S.AUDITOR are created.

When they authenticate for the first time, the TOE will prompt them to change the default password created during initialization.

7.7 Security Audit (FAU)

FAU_GEN.1 Audit data generation

Entrust PKI Hub 1.0.0 keeps information on the operations performed by maintaining events logs. Recorded Operations include those done by the administrators or the requestors of the OCSP and time-stamping services, as well as operations executed internally by services installed with the product. Some examples of logged operations are the signature of an OCSP response, a change in the OCSP configuration, the signature of a timestamp token, or a change in the timestamp configuration.

Operations are divided into events, so that information on one or more events is stored for each relevant operation. Both informative and error events are logged. Event information is stored in the Grafana Loki database. Grafana Loki is a set of components embedded in fcs that implement a fully logging stack (see Grafana Loki documentation | Grafana Loki documentation)

The TOE is able to generate an audit record with the following auditable events:

a) Start-up and shutdown of the audit functions. The audit functions are always started/stopped when the PKI Hub services are started/stopped. It is not possible with PKI Hub to start only the Audit Data Generation services without to start the PKI Hub services. When PKI Hub services start, an audit record is generated in the Loki database, and when the PKI Hub services shutdown then also an audit record is generated indicated that PKI Hub and the solutions deployed have been stopped.
b) The following auditable events
    a. TOE initialization. The Audit Generation Function generates a log entry when the TOE is initialized.
    b. TOE start-up. The Audit Generation Function generates a log entry when the TOE is started-up.
    c. Start of OCSP service operation.
    d. Stop of OCSP service operation.
    e. Generation of OB.OCSP_KEY_PUB and OB.OCSP_KEY_PRIV pairs.
    f. Destruction of OB.OCSP_KEY_PUB and OB.OCSP_KEY_PRIV pairs.
    g. OCSP generation.
    h. Start of TSU operation.
    i. Stop of TSU operation.
    j. Generation of OB.TST_KEY_PUB and OB.TST_KEY_PRIV pairs.
    k. Destruction of OB.TST_KEY_PUB and OB.TST_KEY_PRIV pairs.
    l. Time-stamp generation.
    m. Users and roles management operations. During TOE is initialization, the S.OFFICER and S.AUDITOR users are created with default credentials. As part of the initialization, the Security Officer and the Auditor must change their passwords. Those password changes and any other later password change are registered by the Audit Data Generation function in audit logs.
    n. Successful and unsuccessful operations, including
        i. Attempts of initiating a user session. The Audit Data Generation Function register all the attempts (successful and unsuccessful) to access of initiating a user session; these attempts imply to use the user authentication mechanism (user/password).

ii. Access to the security attributes of the TOE OB.OCSP_CONTEXT. The Audit Data Generation Function register all the attempts (successful and unsuccessful) to access the security attributes of the TOE OB.OCSP_CONTEXT; these attempts imply to use the user authentication mechanism (user/password) and can be done by an external user or by internal service.
iii. Access to the security attributes of the TOE OB.TST_CONTEXT. The Audit Data Generation Function register all the attempts (successful and unsuccessful) to access the security attributes of the TOE OB.TST_CONTEXT; these attempts imply to use the user authentication mechanism (user/password) and can be done by an external user or by internal service.
iv. Unsuccessful attempts to access the TOE resources. The Audit Data Generation Function register all the unsuccessful attempts to access the TOE resources; these attempts imply to use the user authentication mechanism (user/password) and can be done by an external user or by internal service.

o. Value changes in OB.OCSP_CONTEXT. The Audit Generation Function generates a log entry for each changes to the configuration of the TSF.
p. Value changes in OB.TST_CONTEXT. The Audit Generation Function generates a log entry for each changes to the configuration of the TSF.
q. Last successful synchronization check. The Audit Generation Function generates a log entry for each time that PKI Hub (via `chrony` component) synchronizes the internal clock with the UTC received from the configured external NTP servers.
r. Manual synchronization (date of synchronization operation and value of synchronization correction),]. The Audit Generation Function generates a log entry for each time that Security Officer synchronizes manually (via `chrony` component) the internal clock with the UTC received from the configured external NTP servers.

The TOE Audit Data Generation Function is able to generate an Audit record with the following audit information:

- Date and time when the event occurred
- Identification of the entity (user or service) that generated the event
- Identification for the type of the event

- For certain events, a number that uniquely identifies all the events related to the same operation
- Importance of the event. Logs are classified in the following categories according to their importance:
    - Informational: events of this category provide information in operations that were successfully performed
    - Warning: indicates that an unusual condition was detected during an operation, but this did not cause the operation fail
    - Error: indicates that an operation failed due to a predictable error. This category implies a failure operation
- A string describing the event and a list of parameters whose value will vary depending on the data over which the operation was executed.

FAU_SAR.1 Audit review; FAU_SAR.3 Selectable audit review

PKI Hub provides an interface to allow Auditor to read the audit logs stored in the embedded Grafana Loki database. These audit records are presented in a human-readable format that allows the information to be interpreted.

The PKI Hub component that displays those audit records is Grafana (see Grafana | Query, visualize, alerting observability platform). Grafana is an observability and data visualization platform that allows to query, visualize, alert on and explore logs.

Grafana provides a GUI to explore the logs. Grafana provides options for:

- Searching, sorting and ordering the logs. Grafana makes use of LogQL (see LogQL: Log query language | Grafana Loki documentation) that allows complex queries involving field extraction, regular expressions, and pattern matching.
- Customize how logs are displayed
- Watch log streams live.

FAU_STG.2 Guarantees of audit data availability; FAU_STG.4 Prevention of audit data loss

Event information is stored in the Grafana Loki database embedded in PKI Hub. The database files are stored in the OS, protected with `root` OS permissions. OS access controls in the operating environment prevent audit records from being deleted, modified, or added by unauthorized users.

Older logs are overwritten in case the audit trail is about to fill up. This prevents an error from occurring when writing a new log because the Loki database is out of space.

7.8 TOE Policies

The TOE implements the following management policies.

7.8.1 Context Management Policy

The TOE support the administration and enforcement of a OCSP and time-stamp context management policy that provides the capabilities described below.

Subjects (human users) will be granted access to OCSP and time-stamp context objects based upon the:

- Identity of the subject requesting access,
- Role (or roles) the subject is authorized to assume,

Subject identification includes:

- Individuals with different access authorizations
- Roles with different access authorizations

Access type, with explicit allow or deny:

- Read
- Write

7.8.2 Key Management Policy

The OCSP service context (OB.OCSP_CONTEXT) is initially in a non-operational state and it includes no private key. Only the S.OFFICER can generate the private key by means of the `evactl create-key` command. As explained in the FCS section above, this command just triggers the corresponding action to create the key in the HSM. As a result of that creation process, the AT.OCSP_PRIVATE_KEY_VALUE is initialized to the reference of the private key within the HSM. At this point, the context is still in a non-operational state, but with AT.NON_OPERATIONAL_OCSP_CONTEXT_KEY_PAIR_CREATED attribute indicating that the key pair has been created.

An output of the `create-key` command is a CSR that contains the value of the corresponding public key. The user should use this CSR to generate a valid certificate and then update the OCSP service configuration to point to a PEM formatted version of such certificate. Once that operation is completed and if the

certificate public key (AT.IMPORTED_OCSP_CERTIFICATE_PUBLIC_KEY) matches with the one currently configured in the OCSP service context, the AT.IMPORTED_PCS_CERTIFICATE will be set to the value of the just imported certificate.

Only the S.OFFICER can destroy the private key by means of the `evactl` CLI `delete-key` command. As explained in the FCS section above, this command just triggers the corresponding action to delete the key from the HSM. If the private key that's been destroyed is the one referenced by AT.OCSP_PRIVATE_KEY_VALUE, the context will get back to a non-operational state.

The TSU context (OB.TST_CONTEXT) is initially in a non-operational state and it includes no private key. Only the S.OFFICER can generate the private key by means of the `tsactl create-key` command. As explained in the FCS section above, this command just triggers the corresponding action to create the key in the HSM. As a result of that creation process, the AT.TST_PRIVATE_KEY_VALUE is initialized to the reference of the private key within the HSM. At this point, the context is still in a non-operational state, but with AT.NON_OPERATIONAL_TST_CONTEXT_KEY_PAIR_CREATED attribute indicating that the key pair has been created.

An output of the `create-key` command is a CSR that contains the value of the corresponding public key. The user should use this CSR to generate a valid certificate and then update the TSU configuration to point to a PEM formatted version of such certificate. Once that operation is completed and if the certificate public key (AT.IMPORTED_TIMESATMP_CERTIFICATE_PUBLIC_KEY) matches with the one currently configured in the TSU context, the AT.IMPORTED_TST_CERTIFICATE will be set to the value of the just imported certificate.

7.8.3 OCSP Response Generation Policy

When the OCSP service receives an OCSP request (OB.OCSP_REQUEST), it first checks that the request is valid (well-formatted). If it's not valid, it will generate an OCSP error response and stop the processing.

If the request is valid, the OCSP response (OB.OCSP_RESPONSE) is generated following these steps:

- If the certificate whose status has been requested is not found in the database, an `unknown`, `good` or `revoked` status response is returned depending on the OCSP policy that is in use. When `revoked` is returned, the revocation date is set to "Jan 1st 00:00:00 1970 GMT".

- If the certificate is found in the database, either a `good` or `revoked` status response is returned, according to the status found in the database. The revocation date and other details are also informed in the response.
- If the `nonce` extension (AT.OCSP_REQUEST_NONCE) is present in the request and the OCSP policy includes copying the extension into the response, it is copied into the `nonce` extension of the response.
- The value of the internal clock (AT. DATE_AND_TIME_VALUE) is set into the `producedAt` field of the response (AT.OCSP_RESPONSE_TIME).
- The resulting structure is digitally signed using the OCSP service private key (residing in the HSM and referenced by AT.OCSP_PRIVATE_KEY_VALUE).

7.8.4 Timestamp Token Generation Policy

When the TSU receives a timestamp request (OB.TST_REQUEST), it first checks that the request is valid (well-formatted). If it's not valid, it will generate an error response and stop the processing.

If the request is valid, it will check the time-stamping policy that has been requested (AT.REQUEST_POLICY_IDENTIFIER), if any. If it's not a valid policy, an error response will be generated and the processing will end.

Then the hash algorithm is also checked (AT.HASH_ALGORITHM_IDENTIFIER). Only the valid hash algorithms supported by the TSU will be allowed. Moreover, the length of the digest needs to be consistent with the chosen hash algorithm.

At this point, all checks on the request are completed.

So next thing that is checked is that the internal clock (OB. DATE_AND_TIME) reported deviation from UTC is within the accuracy required by the current policy. If the deviation is greater than the supported accuracy, a `TimeNotAvailable` error response is generated.

If clock value is considered accurate, then it is used to check that we are within the validity period of the private key configured for the TSU (AT.TST_PRIVATE_KEY_EFFECTIVE_VALIDITY_PERIOD). If we are not, an error response is generated.

If all the previous checks are passed, the timestamp token (OB.TST_TOKEN) is generated following these steps:

- If the `nonce` field (AT.TST_REQUEST_NONCE) is present in the request, it is copied into the `nonce` field of the response.
- If the `messageImprint` field (AT.DATA_IMPRINT) is present in the request, it is copied into the `messageImprint` field of the response.

- A unique `serialNumber` value is generated for the timestamp.
- The value of the internal clock (AT. DATE_AND_TIME_VALUE) is set into the `genTime` field of the response (AT.TST_TOKEN_TIME).
- The resulting structure is digitally signed (AT.TST_TOKEN_SIGNATURE) using the TSU private key (residing in the HSM and referenced by AT.TST_PRIVATE_KEY_VALUE).

8 Bibliography and acronyms

For the purposes of this document, the symbols, abbreviations, terms and definitions given in [CEN 419 231] and [eIDAS] article 3 apply.

8.1 Bibliography

The following documents are referenced in this document:

Reference	*Referenced document*
[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.
[ISO/IEC 15408-2]	ISO/IEC 15408-2:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components.
[ISO/IEC 15408-3]	ISO/IEC 15408-3:2008 Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components.
[ISO/IEC 15408]	ISO/IEC 15408, Information technology - Security techniques - Evaluation criteria for IT security.
[EN319421]	EN 319 421 Electronic Signatures and Infrastructures (ESI) - Policy and Security Requirements for Trust Service Providers providing Time-Stamping Services.
[FIPS PUB 140-2]	FIPS PUB 140-2, Security requirements for cryptographic modules.
[ISO/IEC 19790]	ISO/IEC 19790:2006, Information technology – Security techniques – Security requirements for cryptographic modules.
[CEN TS 419 221-2]	CEN EN 419 221-2. Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup.
[CEN TS 419 221-4]	CEN EN 419 221-4. Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup.
[CEN TS 419 221-5]	CEN EN 419 221-5. Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services.
[ETSI 119 312]	ETSI TS 119 312. Electronic Signatures and Infrastructures (ESI); Cryptographic Suites for Secure Electronic Signatures.
[ETSI 319 411-2]	ETSI EN 319 411-2. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
[SOG-IS-Crypto]	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms. SOG-IS Crypto Working Group.
[CEN 419 231]	CEN EN 419 231:2013. Protection profile for trustworthy systems supporting time stamping.

8.2 Acronyms

The following abbreviations are used in this document:

Acronym	*Meaning*
CA	Certification Authority
RA	Registration Authority
CSR	Certificate Signing Request
CP	Certificate Policy
ETSI	European Telecommunications Standards Institute
CEN	Comité Européen de Normalisation (European Committee for Standardization)
HSM	Hardware Security Module
VA	Validation Authority
TSP	Trust Service Provider
TWS	Trustworthy System
PP	Protection Profile
ST	Security Target
EAL	Evaluation Assurance Level
TOE	Target Of Evaluation
TSF	TOE Security Function
SFR	Security Functional Requirements
SFP	Security Function Policy
OSP	Organizational Security Policy
TSP	Trust Service Provider
TC	Technical Committee
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
CC	Common Criteria, ISO/IEC 15408, Evaluation criteria for IT security
PKI	Public Key Infrastructure
TLS	Transport Layer Security
LoA	Level of Assurance