Security Target for vinCERTcore 4.0.5.5733

Evaluation according to Common Criteria EAL4+

Version: 1.12
Date: 05/03/2018

vintegris
INFORMATION SECURITY

vintegris.com

Table of Contents

1. Security Target introduction 4
1.1. Security Target Reference 4
1.2. TOE reference 4
1.3. Acronyms 5
1.4. TOE overview 6
1.4.1. TOE type and usage 6
1.4.2. Security Features 6
1.4.3. Non TOE hardware/software/firmware requirements 8
1.5. TOE description 8
1.5.1. Physical scope of the TOE 8
1.5.2. Logical scope of the TOE 9
2. Conformance claims 16
3. Security Problem Definition 17
3.1. Organizational Security Policies 17
3.2. Context definition 18
3.3. Threats 19
3.4. Assumptions 20
4. Security Objectives 21
4.1. Security Objectives for the TOE 21
4.2. Security Objectives for the Operational Environment 22
4.3. Security Objectives Rationale 23
4.3.1. Tracing between security objectives and the security problem definition 23
4.3.2. Justification for the tracing 24
4.4. Conclusion 27
5. Security requirements 28
5.1. Security Functional Requirements 29
5.1.1. Security Audit (FAU) 29
5.1.2. Cryptographic support (FCS) 32
5.1.3. User data protection (FDP) 33
5.1.4. Identification and authentication (FIA) 49
5.1.5. Security management (FMT) 52
5.1.6. Protection of the TSF (FPT) 54
5.1.7. TOE access (FTA) 54
5.1.8. Trusted path/channels (FTP) 55
5.2. Security Assurance Requirements 56
5.3. Security Requirements Rationale 59
5.3.1. Security Requirements Coverage 59
5.3.2. Security Requirements tracing justification 61
5.3.3. Rationale for EAL4 augmented 65
6. TOE summary specification 66
6.1. Identification and authentication (TSF.IA) 66
6.2. Roles (TSF.Role) 68
6.3. Certificate and key-pair lifecycle (TSF.CertSign) 69
6.3.1. Key protection 69
6.3.2. Certificate lifecycle 70
6.3.3. Signature delegation 76
6.3.4. Secure signature 79
6.4. Audit (TSF.Audit) 81
6.4.1. Audit generation and storage 81
6.4.2. Audit access control and review 82
6.4.3. Audit archiving and verification 83
6.4.4. Audit analysis and warning notifications 84
6.5. Admin functions (TSF.Admin) 85
6.5.1. Configure environment and security 86
6.5.2. Audit purge 87
6.5.3. Infrastructure and control keys management 87
6.6. Backup and restore (TSF.Backup) 89

6.6.1. Backup and restore access control 89
6.6.2. Backup generation 89
6.6.3. Restore system 90
6.7. Secure communications and session management (TSF.Comm) 91
6.8. Secure start-up and self-test (TSF.Start) 93
7. References 94
Annex A. Terms, definitions and abbreviations 95

List of Figures

Figure 1: Logical scope of the TOE 9
Figure 2: internal TOE subsystems 10
Figure 3: Identification and Authentication 11
Figure 4: Cryptography 12
Figure 5: Certificate management 13
Figure 6: TOE management 14
Figure 7: Audit generation and review 15

List of tables

Table 1: TOE requirements 8
Table 2: Organizational Security Policies 17
Table 3: TOE assets 18
Table 4: TOE user subjects 18
Table 5: TOE threat agents 19
Table 6: TOE threats 19
Table 7: Assumptions 20
Table 8: Tracing between security objectives and the security problem definition 23
Table 9: Audit events 30
Table 10: Access control policy summary 34
Table 11: Subject security attributes 37
Table 12: Object security attributes 38
Table 13: TOE user attributes 49
Table 14: Function/Role mapping 52
Table 15: Assurance requirements for EAL4+ ALC_FLR.2 56
Table 16: SFR dependency satisfaction mapping 58
Table 17: Security Requirements Coverage 60
Table 18: SFRs related to Identification and authentication 67
Table 19: SFRs related to Roles 68
Table 20: SFRs related to Key protection 69
Table 21: SFRs related to Certificate lifecycle 75
Table 22: SFRs related to signature delegation 78
Table 23: SFRs related to signature creation 80
Table 24: SFRs related to audit storage 82
Table 25: SFRs related to audit review 83
Table 26: SFRs related to audit archiving and verification 83
Table 27: SFRs related to audit analysis and warnings 84
Table 28: SFRs related to admin functions 85
Table 29: SFRs related to configure environment and configure security 86
Table 30: SFRs related to audit purge 87
Table 31: SFRs related to key regeneration 88
Table 32: SFRs related to backup and restore access control 89
Table 33: SFRs related to backup generation 89
Table 34: SFRs related to restore system 90
Table 35: SFRs related to secure communications 92
Table 36: SFRs related to start-up and self-test 93

1. Security Target introduction

This Security Target describes the security objectives and security requirements for vinCERTcore version 4.0. The specifications are consistent with the Common Criteria for Information Technology Security Evaluation, Version 3.1([1], [2] and [3]).

1.1. Security Target Reference

Document identification	Security Target for vinCERTcore 4.0.5.5733
Version	1.12
Autor	Víntegris S.L.
Date	5th February, 2018

1.2. TOE reference

TOE identification	**vinCERTcore**
Version	**4.0.5.5733**
Autor	Víntegris S.L.
CC Identification	Common Criteria for Information Technology Security Evaluation v3.1 R4
Assurance level	**EAL4+ACL_FLR.2**

1.3.Acronyms

AdES	Advanced Electronic Signature
CC	Common Criteria, ISO/IEC 15408, Evaluation criteria for IT security
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CEN/ISSS	CEN Information Society Standardization System
CSP	Certification Service Provider
DTBS	Data to be Signed
EAL	Evaluation Assurance Level
EC	European Commission
EESSI	European Electronic Signature Standardization Initiative
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISSS	Information Society Standardization System
PIN	Personal Identification Number
PKC	Public Key Certificate
QC	Qualified Certificate
QES	Qualified Electronic Signature
SAD	Signer's Activation Data
SAP	Signature Activation Protocol
SCA	Signature Creation Application
SCD	Signature Creation Data
SCDev	Signature Creation Device
SCDid	Signature Creation Data Identifier
SVD	Signature Validation Data (Representative to Public key)
SD	Signers' Document
SDO	Signed Data Object
SGSP	Signature Generation Service Provider
SSA	Server Signing Application
SSCD	Secure Signature Creation Device
TS	Technical Specifications
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing
VAD	Validation authentication data. Used to enable signature
WS/E- SIGN	CEN/ISSS Electronic Signatures workshop

1.4. TOE overview

The vinCERTcore is a server that provides secure and centralized digital signature and certificate management. It is the central part of nebulaCERT® which is a suite of products that implements a server for remote signing.

1.4.1. TOE type and usage

The TOE type of vinCERTcore is a software server which provides all the functionality for certificate management and centralized digital signature. It uses an external user repository and works with a HSM (out of ST scope) which will hold all the sensible cryptographic material. Additionally it uses a set of external IT products to provide the overall functionality.

The management of certificates of vinCERTcore allows end-users to manage the certificate creation flow in the system using the external vinCERTweb product (out of scope of evaluation) and storing them in the HSM. The operative can be performed in two different ways:

- Importing user's digital certificates.
- Generating new certificates which can be enrolled in an external CA.

The management of certificates of vinCERTcore also allows authorized end-users *delegate* the usage of the certificates. This is accomplished using the related functionalities on vinCERTweb.

It's required a vinCERTagent software (out of scope of evaluation) installed for digital signature purposes. This agent is compatible with CSP and PKCS#11 and it is installed on user's device and transparently, communicates with vinCERTcore allowing users to perform digital signature through it. End users can use any of their allowed certificates which are stored in vinCERTcore. Digital signatures are always performed remotely in the vinCERTcore HSM (out of scope of evaluation). Password protected key usage is also supported.

The vinCERTagent and the vinCERTweb external modules connects to the vinCERTcore in order to authenticate end-users. They present necessary dialogs to allow end-users to perform multiple factor authentication against the Active Directory and the Radius Server (both external to the TOE).

The administration of the TOE (vinCERTcore) is performed using an SSH console connected to the TOE by Active Directory users with privileged role. Once single-factor has been satisfied, they are allowed to start the TOE on maintenance mode which permits the sensitive operatives such as configuration management, backup and restores and audit data review and export.

1.4.2. Security Features

The implementation of the TOE (vinCERTcore) is focused but not limited to the following secure aspects of the product.

Authentication and Authorization:

The TOE implements different authentication levels processing data to/from Active Directory and a second factor authentication based on RADIUS server. The vinCERTcore uses the following roles in order to manage access control to system functionalities: Signer, Certificate Owner, Administrator, Operator, Auditor and Security Officer.
Two factor authentication is required to sign with vinCERTagent and manage certificate lifecycle with vinCERTweb. Simple factor authentication is required to perform administrative operations with an SSH client.

Key Usage:

The usage of keys to perform cryptographic operations (mainly signing operations) is protected by usage policies implemented within the TOE and managed through the vinCERTweb product. It can be also protected by a key activation password required at the moment of signature performing. The TOE allows Certificate Owner to delegate *signature creation* to another signer.

Key Management:

The TOE manages sensitive keys stored in HSM. The access to these keys is protected by a credential managed by the TOE. This ensures that the TOE users only can manage their associated keys and they are always safe and cannot be accessed by other entities than the TOE itself.

Audit:

All TOE operations related to keys are stored in a secured audit trail along which always grow and cannot be tampered nor deleted unless exported by a qualified environment's Auditor.
The exported audit data can be used as a legal evidence of the performed signatures.

Backup and restore:

The TOE data can be backed up in order to be restored later. This allows to prevent data and functionality loss in case of disasters.

1.4.3. Non TOE hardware/software/firmware requirements

The following requirements are the elements of the TOE environment, out of the scope to the TOE that requires and relies on.

Type	Description	
Server Machine	Operating system	Windows Server 2012 R2
	CPU	Minimum 3.0 Ghz dual-core processor
	Memory RAM	Minimum 2 GB RAM
	Disc space	Minimum 40 GB
HSM	HSM (i.e. THALES nShield) compliant with CENT/TS 419241:2014 SRG_KM1.1 that meets requirements of CWA 14169; or meets the requirements identified in CWA 14167-2, CWA 14167-3 or CWA 14167-4 or is a trustworthy system which is evaluated at EAL 4 or higher in compliance with the ISO/IEC 15408 series, or at an equivalent security criterion or meets the requirements identified in FIPS PUB 140-2, level 3 or higher.	
Database	PostgreSQL 9.4.4 (Minimum version)	
Software	Java 1.8 x64	
User repository	MS Active Directory	
Mail server	SMTPS compatible server	
PKI (CA acting)	vinCERTcamgr (version 4.0.5) server communicating to endpoint PKI CA.	
SSH Client	Software program which uses the secure shell protocol to connect to a remote computer. Must support SSH v.2 protocol.	
Second factor authentication server	RADIUS compatible second factor authentication server	
Signature client	vinCERTagent (version 4.0.5)	
Management frontend	vinCERTweb (version 4.0.5)	

Table 1: TOE requirements

1.5. TOE description

1.5.1. Physical scope of the TOE

The TOE, which is named vinCERTcore, is a software server that is provided as a MSI installable package, once this package is executed a semiautomatic wizard will aid to perform a secured installation and minimal configuration.

Along with the MSI there are also provided guides in PDF format which extensively describes the installation, operation and administration of the TOE for be used by users with privileged roles. The following guides are provided in version:

- AGD_PRE.1 Preparative procedures (v.1.5)
- nebulaCERT-vinCERTcore-Instalacion y configuración (v.1.7)
- nebulaCERT-Entorno-Instalacion y configuración (v.1.7)
- AGD_OPE.1 Operational user guidance (v.1.5)
- nebulaCERT-vinCERTcore-Administracion (v.1.5)
- nebulaCERT-Entorno-Administracion (v.1.5)
- nebulaCERT-Guia de uso (v.1.3)

1.5.2. Logical scope of the TOE

The vinCERTcore is located on the center of the nebulaCERT® suite and it is the central component which implements the main functionality and security. It requires and relies upon a set of external IT products located on the TOE's environment and controlled by the organization personnel.

For a general overview the following figure is provided in order to show how vinCERTcore connects with the external IT products, the TOE is shown in green and the external IT products are shown in blue.

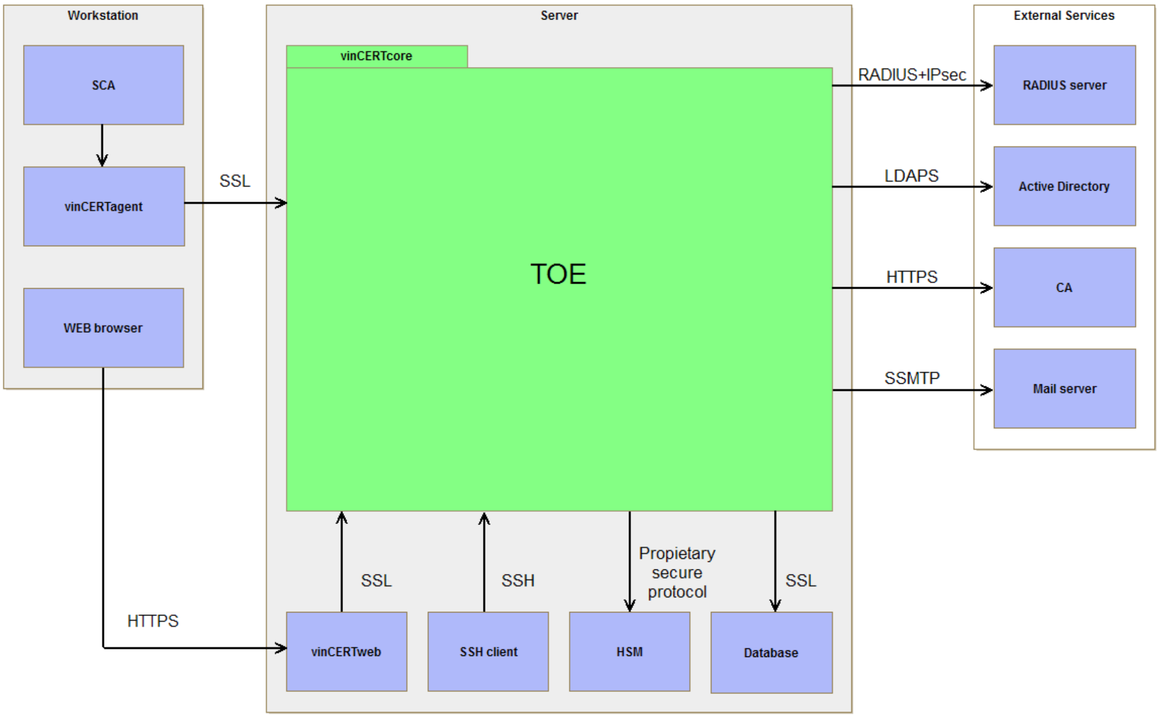

Figure 1: Logical scope of the TOE

The vinCERTagent product is installed on the end-user workstation and it is in charge of providing all cryptography functionalities transparently to the operating system, it is done by securely connecting with vinCERTcore. When an SCA in the end-user workstation is using such OS cryptography features it is transparently using nebulaCERT®.

The end-user disposes vinCERTweb product which securely connects to vinCERTcore and presents him the certificate managing features. The end-user shall use a web browser to securely access (HTTPS only) to vinCERTweb.

For administering vinCERTcore the organization personnel shall use an SSH client inside the server which hosts the TOE and connect to it.

vinCERTcore uses two local services which are installed on the same server as the TOE: The HSM (or its middleware) and the Database. For the rest of services the TOE must be configured to connect to them through the network. Those services are the RADIUS server, the Active Directory, the remote CA and the Mail server.

Connections between TOE and RADIUS Server, Active Directory, remote CA and Mail Server use secure protocols as shown on the figure 1.

The following figure shows the internal TOE subsystems.

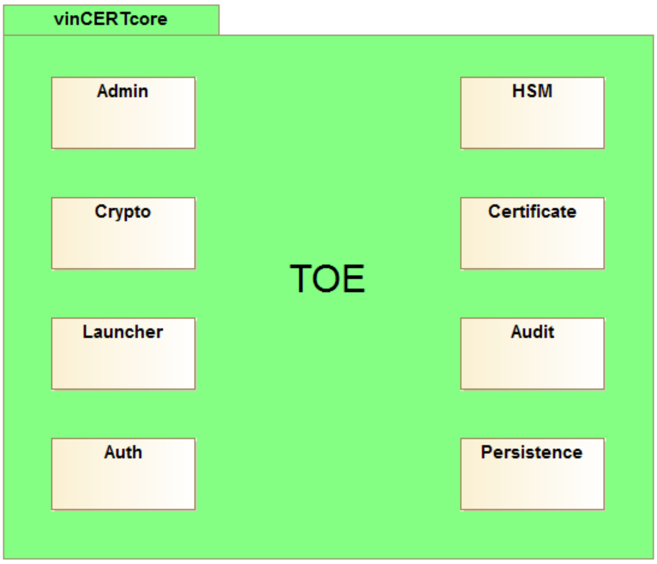

Figure 2: internal TOE subsystems

Admin subsystem provides operations for managing certificates and policies. It exposes an HTTPS service which is used by vinCERTweb.

Crypto subsystem provides operations for requesting signature function to HSM subsystem and the related cryptography. It exposes an HTTPS service which is used by vinCERTagent.

Launcher subsystem is responsible for initiating vinCERTcore and provides an SSH service that allows SSH clients to connect to it in order to perform privileged operations.

Auth subsystem is responsible for centralized user authentication. It permits first factor and second factor authentication mechanisms. Both vinCERTweb and vinCERTagent connects (out of scope of ST) to this subsystem to allow end-user authentication to the TOE.

HSM subsystem is responsible for interacting with the organization's HSM or its respective middleware.

Certificate subsystem holds the operatives of certificate management, policy management and the related security.

Audit subsystem is used to allow the generation of an Audit trail which will be trustworthy and could be used as a legal evidence of signature. It also monitors the actions that occurs in vinCERTcore and is capable of apply countermeasures in case of attack or failure.

Persistence subsystem provides the wrapper functions necessary for let the Database be used by the other TOE subsystems.

1.5.2.1. Description of the TOE internal functionality

Following is the general description of the internal operation of vinCERTcore. It is explained from the point of view of the main functionalities and with the intention to giving a summary of the functionality and security, it isn't an exhaustive description of the TOE internals.

1.5.2.1.1. Identification and Authentication

The identification and authentication of users in vinCERTcore is done using multiple factor procedures, each of them are used in different entrance points.

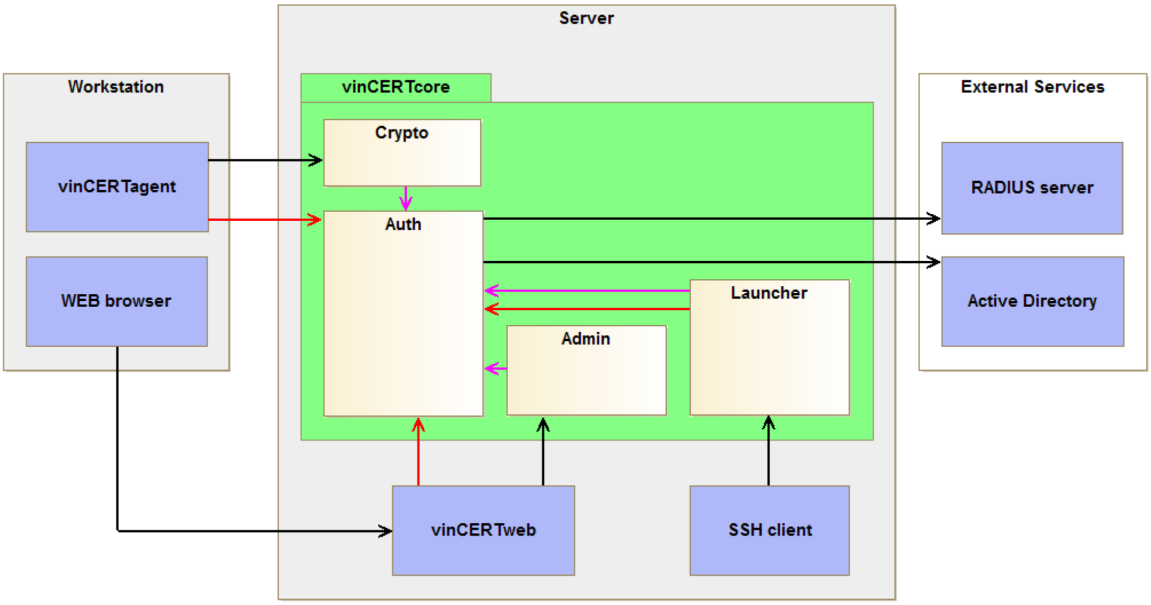

Figure 3: Identification and Authentication

Auth subsystem is in charge of generating nebulaCERT® compatible tickets, those tickets are requested by vinCERTagent and vinCERTweb when the user that is using nebulaCERT® is going to be authenticated, as shown by the red arrows in figure 3 from these products.

When a user uses vinCERTagent or vinCERTweb, their respectively subsystems, Crypto and Admin, present the acquired ticket in order to prove that the end-user is already authenticated, those subsystems internally checks the tickets against Auth subsystem (purple arrows in figure 3). When a privileged user uses an SSH client to connect to vinCERTcore locally in the server, the Launcher subsystem will perform a similar operation acquiring a ticket and verifying that ticket (red and purple arrows in figure 3 from Launcher subsystem).

Auth subsystem uses the external services, Active Directory and RADIUS server, for identification and authentication of users. For authentication from vinCERTagent and vinCERTweb services, a multiple factor authentication will be required. For SSH client authentication a sole factor against Active Directory will be used.

1.5.2.1.2. Cryptography

The vinCERTcore provides remote digital signature and general cryptography functionality to remote users. This way end-users could use their certificates to request cryptographic operations to the TOE.

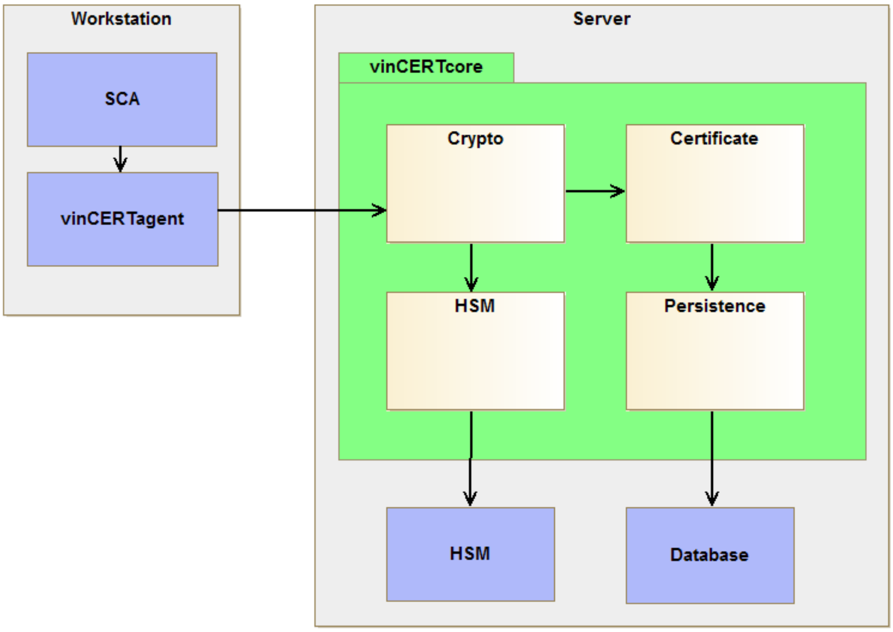

Figure 4: Cryptography

Crypto subsystem is in charge of providing support for cryptographic operations and vinCERTagent is in charge of providing a transparent way for end-users to access this functionality. As shown in the figure 4, an SCA in the end-user workstation accesses to cryptographic operations through vinCERTagent which securely connects to vinCERTcore.

Crypto subsystem uses Certificate subsystem to access certificate policies and security operations. Certificate policies are stored on the external database and are provided by Persistence subsystem. Policies are the means for verify that cryptographic operations are allowed. Crypto subsystem performs the operation through HSM subsystem. The cryptographic operations supports *SAD* generation using user PIN for the activation of the key in the external HSM.

HSM and Persistence subsystems are connectors which presents the external functionalities to the TOE.

1.5.2.1.3. Certificate management

The vinCERTcore provides a web service for vinCERTweb frontend in Admin subsystem. The end-users are allowed to manage their certificates and related policies and delegations into the Admin subsystem.

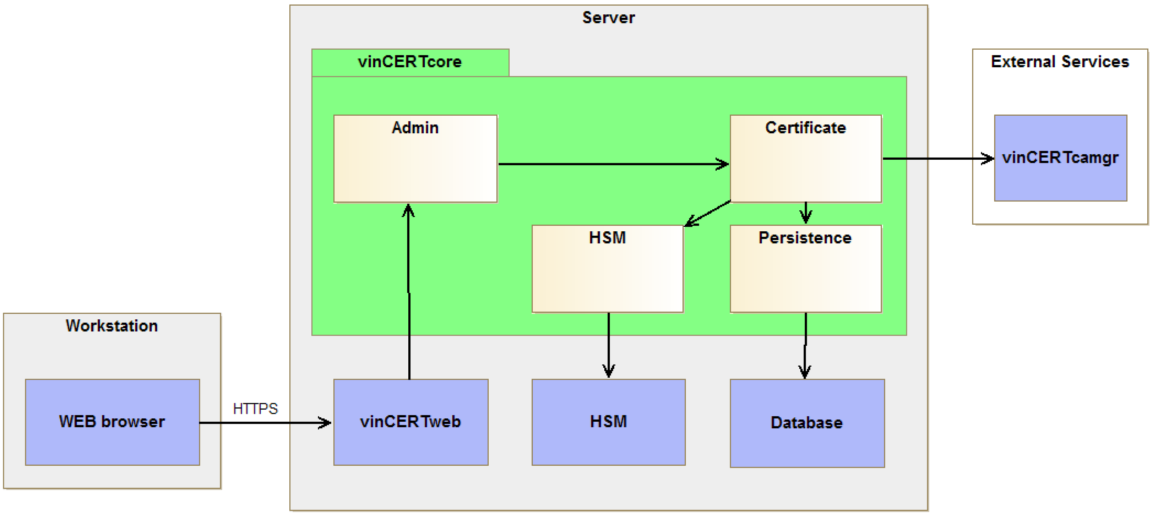

Figure 5: Certificate management

An end-user uses a WEB browser on his workstation to connect in secure way (HTTPS) with the external vinCERTweb module which implements the web frontend. Also, vinCERTweb interacts with vinCERTcore, and provides the entrance to the certificate management functionality of Admin subsystem.

Admin subsystem works with Certificate subsystem which is in charge of performing the certificate related operatives. Certificate subsystem uses HSM and Persistence subsystems to manage the data related with certificates. This includes cryptographic key-pair's generation into the external HSM, and usage policies into the external database.

Certificate subsystem communicates with vinCERTcamgr module, which manages connection to an external CA in order to issue qualified certificates.

1.5.2.1.4. TOE management

The vinCERTcore is managed by the administration personnel from the same server in which is installed.

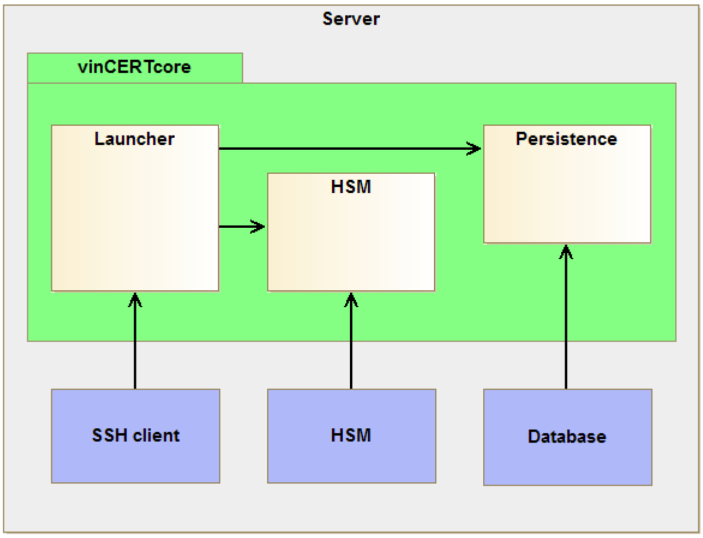

Figure 6: TOE management

The administrator personnel uses an SSH client to connect to Launcher subsystem and to carry out administration operatives.

Launcher subsystem manages the vinCERTcore configuration, the internal infrastructure and control keys and the overall internal data protection using signature and encryption. This protections are done through the HSM subsystem towards HSM server. Management integrity and confidentiality data in database it's done through the Persistence subsystem towards the external database.

1.5.2.1.5. Audit generation and review

The vinCERTcore audit functionality generates verifiable data that can be used to provide legal proof of the cryptographic operations. An auditor user can use vinCERTcore to review the generated audit data.

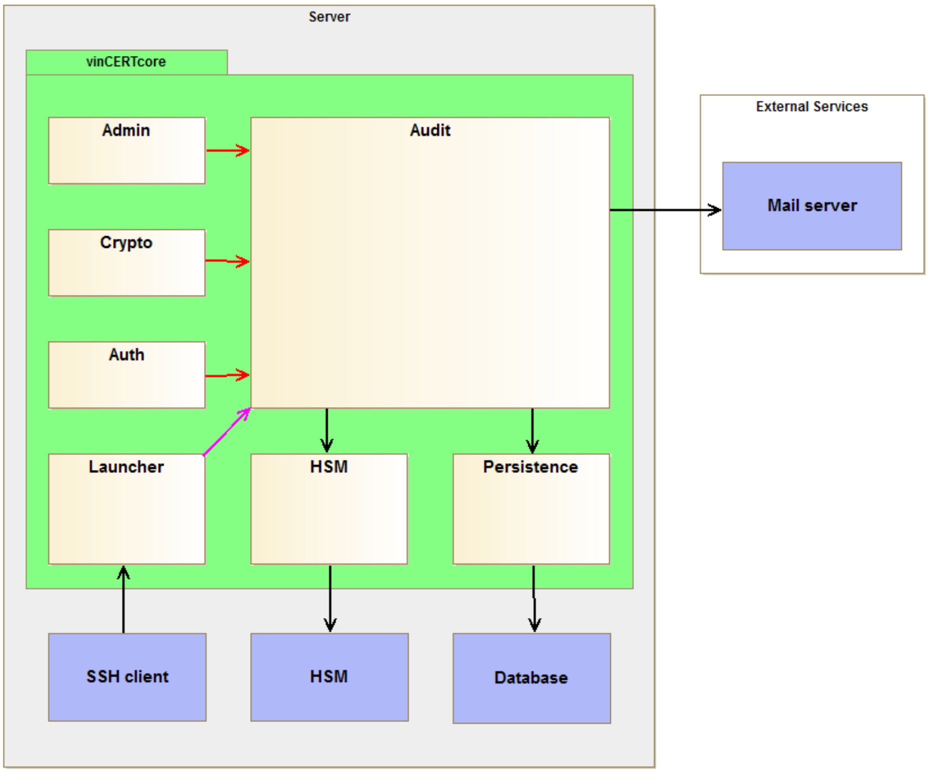

Figure 7: Audit generation and review

The origin of the audit data in vinCERTcore starts in the business logic modules contained inside the subsystems which exposes external functionalities. These subsystems are the Admin subsystem, the Crypto subsystem, the Auth subsystem and the Launcher subsystem.

They originate audit data and asks to Audit subsystem to generate an *Audit registry*, this is shown by the red arrows and the purple arrow in the figure 7 and it is done at each relevant operation regarding signature, management and security operations. The Audit subsystem also uses the system's Time Source to add a Time Stamp on the generated *Audit registry*.

The Audit subsystem uses HSM and Persistence subsystems to generate a verifiable and unmodifiable *Audit trail*. Each *Audit registry* of *Audit trail* is signed using the external HSM and concatenated with previous. *Audit trail* is stored on the external database.

Also, Audit subsystem is in charge of detecting potential security breaches and attacks. When one is detected, the subsystem takes different measures to preserve the security.

Through an SSH client, a privileged user with the *Auditor* role can use the vinCERTcore audit functionalities to browse and review the current *Audit trail*. The Administrator and Operator roles could also export the current *Audit trail* so it can be presented and reviewed outside the TOE. This operations are done by the Launcher subsystem against the Audit subsystem as shown by the purple arrow.

2. Conformance claims

The vinCERTcore Security Target and this TOE are conformant to the following CC specifications:

- Common Criteria for information Technology Security Evaluation, Part 2: Security functional components, September 2012, Version 3.1 revision 4 [2].

- Common Criteria for information Technology Security Evaluation, Part 3: Security assurance components, September 2012, Version 3.1 revision 4 [3].

The vinCERTcore Security Target and the TOE not claim conformance with any Protection Profile.

The vinCERTcore Security Target is conformant to assurance level EAL4 augmented with **ALC_FLR.2** defined in:

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

3. Security Problem Definition

3.1. Organizational Security Policies

Organization Security Policy	Description
P.Crypto_Managment	S.SecurityOfficer will maintain the TOE cryptography strength within an acceptable level based on risk assessment, this means that: • He will change the Infrastructure and Control KEYs with the necessary regularity. • He will change the key algorithms and key lengths if they become unsuitable. • He will change the compromised or suspected to be compromised keys. • He will apply a configuration using only algorithms and algorithm parameters defined by the ETSI/TS 102 176 [6] series for TOE SCD setup.
P.Standard_Time_Source	The TOE uses the system time where it is installed as a Time Source. To ensure the accuracy of the System Time Source, system clock must be set by Organization Administrators, who are responsible for the proper maintenance of system clock.
P.HSM_Backup	The TOE expects that Organization's S.Operator or S.Administrator be in charge of the HSM backup procedures. Those backup procedures will be subjected to the following restrictions: • All HSM keys will be stored in a protected state. • If any key is exported from the HSM, it will be protected to ensure its confidentiality and integrity to the same or higher security level as within the HSM. Wherever the key is protected by encryption, only cryptographic algorithms and algorithm parameters of equivalent or higher strength will be used. • Backup, storage and restoration of keys in the HSM are only performed by authorized personnel. Master keys used to protect both user and working keys shall be backed up, stored and reloaded under at least dual control. Such master keys will only be held outside the HSM in protected form.
P.Audit_Review	Authorized auditor(s) regularly review audit records produced by the TOE, respond promptly to any indication of an attempted or actual security issues.
P.Storage_Review	Organization's personnel must prevent system's storage exhaustion.

Table 2: Organizational Security Policies

3.2.Context definition

This section intends to provide a context for the definition of the entire chapter, it is provided a description of assets, subjects and threat agents.

Assets

Name	Description
SCD	Users signing private key. It either could be used to generate AdES or QES signature.
SVD	Users verifying public key. It is associated to an SCD and is either kept in the DB and in the HSM together with its SCD.
DTBS and DTBS/R	Set of data as data object, document or its representation (hash), to be signed by the signatory and transmitted to the TOE to have a signed object.
Generated digital signature	Is a signed electronic message associating a Document hash with a Signatory's SVD.
Signature-creation function	Signature-creation function of the TOE to create digital signature for the DTBS/R with the SCD.
OTP VAD	Static password as well as OTP entered by the End User to authenticate the user prior to performing a signature operation.
Static VAD	PIN that protects the access to a SCD to assure the sole control of the user.
KEY password	Password that protects the access to a KEY.
SAD	Data used to activate Private Keys (SCD, Control and Infrastructure Keys) on the HSM, it could be generated dynamically inside the TOE using the PIN and other material held by the TOE.
KEY	Infrastructure or control key used by the TOE for internal purposes.
TOE configuration	Configuration parameters that regulate the application of TSF and the strength of the cryptographic material.
Audit data	Audit data that demonstrates the existence of a user action in a concrete date, it could also show attacks or traces of attacks.
Exported audit archive	Set of mechanisms and data intended to provide integrity to an archive that contains audit records.
Exported backup archive	Set of mechanisms and data intended to provide integrity and confidentiality to an archive that contains backup files.

Table 3: TOE assets

User Subjects

Subjects	Description
S.User	End user of the TOE.
S.Signer	S.User that can use the signature functionality of the TOE either using its owned certificates or using delegated ones.
S.CertOwner	S.User who owns certificates.
S.Auditor	Consults the audit trail to monitor the use of certificates and the use of the system.
S.Administrator	Carries out the overall system management.
S.Operator	Performs backup and recovery operations, starts and stops the TW4S and monitors the Server status.
S.SecurityOfficer	S.User that is responsible for administering the security of the TOE and its configuration.

Table 4: TOE user subjects

Threat agents

Threat agents	Description
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. Examples of this threat agent are: unauthorized TOE personnel, cybercriminals, and hackers in general.

Table 5: TOE threat agents

3.3.Threats

Threat	Description	Threatened assets
T.Key_Divulg	An attacker may steal SCDs and/or KEYs and thus make unauthorized use of them.	SCD, KEY, SAD
T.SigF_Misuse	An attacker misuses the signature-creation function of the TOE to create digital signature for data the signatory has not decided to sign.	Signature-creation function, OTP VAD, Static VAD, DTBS and DTBS/R
T.User_Impersonation	A threat agent may gain access to User credentials or use tampering techniques to impersonate him, then he can use functions permitted to the victim that are forbidden to the threat agent	OTP VAD, Static VAD, SAD, KEY password
T.Sig_Forgery	Without use of the SCD an attacker forges data with associated digital signature and the verification of the digital signature by the SVD does not detect the forgery.	Generated digital signature, SVD
T.Config_Access	A threat agent may modify the TOE configuration provoking malfunctions or deliberately change of security parameters that may compromise the correct operation of TSF.	TOE security configuration
T.Audit_Access	A threat agent may access the audit data and either read it without permission, modify it, delete it, or denying its generation; so attacks or signature related events could be concealed. In this threat it is also considered the possibility for an external effect to deny the audit data generation (e.g.: Storage exhaustion).	Audit data
T.Audit_Archive	A threat agent may alter the audit data inside an audit archive so important events in the archive could be changed or deleted.	Audit data, Exported audit archive
T.Backup_Archive	A threat agent may alter the Backup data inside a Backup archive. This can lead in malfunctions or TSF operation fail when the Backup is restored.	Exported backup archive, TOE security configuration

Table 6: TOE threats

3.4. Assumptions

Assumption	Description
A.Trained&Trusted	It is assumed that all TOE users are sufficiently trained in order to operate the TOE securely. It is assumed in addition that every TOE privileged role, including *R.Administrator*, *R.Operator*, *R.SecurityOfficer* and *R.Auditor*, are trusted and not malicious towards the system.
A.No_Malware	It is assumed that no malware will be able to attack the TOE directly from the same operating system.
A.Configuration	It is assumed that the TOE will be properly installed and configured according to the vinCERT Administration Guide and vinCERT Installation Guide. The TOE is considered well configured when all internal tests are successfully executed. The initial tests covers connection to all external products.
A.Trusted_IT_Products	It is assumed that the following external IT products which the TOE communicates with are trusted and reliable. Also the personnel responsible for its administration is trusted and not malicious towards the system: - HSM - PKI *(vinCERTcamgr)* - AD - RADIUS - DB - SMTPS
A.Trusted_Agents	It is assumed that the product's external components *vinCERTagent*, *vinCERTweb* and the O.S. on which these ones operate are trusted and not malicious towards the system.
A.Trusted_O.S.	It is assumed that the O.S. on which the TOE is running is trusted and not malicious towards the system in any way.
A.Trusted_SCA	It is assumed that the signatory will use only a trustworthy SCA. The SCA creates and sends the DTBS or the DTBS/R the R.Signer wishes to sign in an appropriated form to be signed by the TOE. It is also implemented in compliance with functional requirements of CWA 14170 [7].
A.Certified_HSM	It is assumed that the HSM component will be hardware based and It'll meet the requirements identified in **EN 419241** [4] and/or will be a trustworthy system which is assured to EAL 4+ or higher in accordance to ISO/IEC 15408, or equivalent security criteria, or will meet the requirements identified in FIPS PUB 140-2 level 3 or higher.
A.No_Physical_Access	It is assumed that no thread agents and users have direct physical access to the TOE

Table 7: Assumptions

4. Security Objectives

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

4.1. Security Objectives for the TOE

OT.Startup&Shutdown_Security TOE secure start-up and shutdown

The TOE performs a secure start-up, being careful of loading the encrypted configuration and starting all modules in the right order and without any errors, and ensuring the mode selected (management / operational) is initiated properly. If any error is detected on start-up process, this one will be aborted, especially for audit module related errors. On shutdown, the TOE must stop its functionality in a secure way, ensuring no audit data is lost or not stored properly before shutting down.

OT.SCD_Secure_Lifecycle Security on SCD creation and destruction

The TOE shall ensure the security of the creation and destruction processes of the SCD, it also shall enforce the protection of the access to the related operatives.

OT.Key_Secure_Management Security on infrastructure and controls KEY management

The TOE shall protect the security of infrastructure and control KEYs in the processes of generation and regeneration, it also shall enforce the protection of the access to the related operatives.

OT.SigFunction_Usage Signature creation function for the legitimate signatory

The TOE provides the signature generation function for the legitimate signatory only and protects the SCD against unauthorized digital signature and general access, this include user-SCD bindings and SCD delegations between R.CertOwner and R.Signer.

OT.Signatory_Auth Signatory authentication based on multifactor authentication

The TOE will strongly authenticate the signatory prior to access signature functions. The authentication will be two factor based composed by a password and an OTP dynamic password. Only after a successful authentication with an identity, a static password and a One-Time Password, the signatory can digitally sign.

OT.Privileged_Auth Privileged authentication prior to administrative operations

The TOE will authenticate the privileged roles prior to any administrative operation. The privileged roles are: *R.SecurityOfficer*, *R.Operator*, *R.Administrator* and *R.Auditor*.

OT.Secure_Delegation Security on certificate delegation mechanisms

The TOE shall ensure the SCD delegation procedure is performed in a secure way and shall provide mechanisms to revoke the delegations, in the case of a *Qualified Certificate* able to perform *Qualified Electronic Signature* the revocation mechanism shall return the control of the certificate to its owner.

OT.Account_Separation Separation between different user accounts

The TOE must ensure each user has access only to the TOE's operatives he's authorized to, based on his/her role.

OT.Audit_Prot Protection of the audit data

The TOE shall implement mechanisms to prevent unauthorized modifications of Audit data, it also shall generate audit data with associated integrity and will protect the exports of the audit records with integrity. The TOE may also stop its functionality during management or operational usage if a critical error related to audit data generation function is detected.

OT.Backup_Prot Backup data protection

The TOE shall protect the backed up data with integrity and confidentiality so it can be verified on *Restore* operations.

OT.Trusted_Comm Trusted communication with external IT products

The TOE enforces that the communication channels with the external trusted IT products (AD server, vinCERTcamgr, Mail server, vinCERTagent, vinCERTweb, HSM, Database and SSH client) are protected in integrity and confidentiality.

4.2. Security Objectives for the Operational Environment

OE.Competent_Users Competent users and Privilegeds

The operational environment shall ensure that all (human) TOE users and those users managing the operational environment are competent to manage, operate, and use the TOE and to maintain the security and privacy of the data it handles.

OE.Configured Proper installation and configuration of the TOE

The operational environment shall ensure that the TOE will be installed and configured properly for its startup and execution in a secure way.

OE.Secure_Env Secure, trusted and reliable external IT products

The operational environment shall ensure that every external element from which the TOE requires resources are secure, trusted, reliable and non-hostile towards It. Including:

- HSM
- PKI (vinCERTcamgr)
- Active Directory
- RADIUS Authentication Server
- Database
- SMTPS
- vinCERTagent
- vinCERTweb
- O.S. on which the TOE is being executed
- The server on which the TOE is being executed

OE.Secure_SCA SCA compliance with the standards

The SCA used by any *S.User* shall be a trustworthy SCA, not malicious against the TOE or its environment and shall be compliant with CWA 14170 [7] standard.

OE.Audit_Review Review of audit system

The operational environment shall ensure that:

- Audit records produced by the TOE are regularly reviewed.
- Any indication of an attempted or actual security issue is responded to.
- Audit records are regularly archived to prevent audit data storage exhaustion.

OE.Certified_HSM Certified HSM

The operational environment shall ensure that the HSM that will be integrated with the TOE will be hardware based and It'll meet the requirements identified in EN 419241 [4] and/or will be a trustworthy system which is assured to EAL 4+ or higher in accordance to ISO/IEC 15408, or equivalent security criteria, or will meet the requirements identified in FIPS PUB 140-2 level 3 or higher.

OE.Standard_Time_Source Standard time source

The operational environment shall ensure that the Time Source provided from the TOE operating system comes from an organization's standard time source and is managed by the organization Operators.

OE.Secured_RADIUS Trusted communication with RADIUS server

The operational environment shall ensure that the communication channel with the external trusted IT product RADIUS server is protected in integrity and confidentiality.

4.3. Security Objectives Rationale

4.3.1. Tracing between security objectives and the security problem definition

Threads-Policies-Assumptions / Security objectives	OT.Startup&Shutdown_Security	OT.SCD_Secure_Lifecycle	OT.Key_Secure_Management	OT.SigFunction_Usage	OT.Signatory_Auth	OT.Privileged_Auth	OT.Secure_Delegation	OT.Account_Separation	OT.Audit_Prot	OT.Backup_Prot	OT.Trusted_Comm	OE.Competent_Users	OE.Configured	OE.Secure_Env	OE.Secure_SCA	OE.Audit_Review	OE.Certified_HSM	OE.Standard_Time_Source	OE.Secured_RADIUS
T.Key_Divulg		X	X				X				X						X		
T.SigF_Misuse	X			X	X		X	X			X		X	X	X			X	X
T.User_Impersonation	X				X	X		X			X		X	X	X			X	X
T.Sig_Forgery													X				X		
T.Config_Access	X		X			X						X	X				X		
T.Audit_Access	X		X			X			X		X	X	X	X		X	X		
T.Audit_Archive	X								X			X	X				X		
T.Backup_Archive						X				X		X	X				X		
P.Crypto_Managment	X	X	X			X						X	X				X		
P.Standard_Time_Source	X				X	X			X	X		X	X	X				X	
P.HSM_Backup												X		X			X		
P.Audit_Review	X					X			X			X		X		X			
P.Storage_Review												X							
A.Trained&Trusted												X	X						
A.No_Malware												X		X					
A.Configuration													X						
A.Trusted_IT_Products														X					X
A.Trusted_SCA															X				
A.Trusted_Agents														X					
A.Certified_HSM																	X		
A.No_Physical_Access														X					

Table 8: Tracing between security objectives and the security problem definition

The TOE shall ensure the SCD delegation procedure is performed in a secure way and shall provide mechanisms to revoke the delegations, in the case of a *Qualified Certificate* able to perform *Qualified Electronic Signature* the revocation mechanism shall return the control of the certificate to its owner.

4.3.2. Justification for the tracing

Here follows the justification for the above tracing:

4.3.2.1. Threats and Security Objective Sufficiency

T.Key_Divulg	Unauthorized divulgation of SCD and/or KEYs

This threat deals with steal and/or unauthorized divulgation of SCDs and KEYs.
The creation and destruction functions for SCDs are secured by the access control and protection mechanisms enforced by **OT.SCD_Secure_Lifecycle**, likewise generation and regeneration of KEYs are secured by the access control and protection mechanisms enforced by **OT.Key_Secure_Management**.
OT.Secure_Delegation provides mechanisms to ensure that SCD delegation and revoke procedures are performed in a secure way.
In the case of SCD import **OT.Trusted_Comm** additionally assures the integrity and confidentiality of SCDs when they're imported to the TOE.
OE.Certified_HSM preserves the SCDs and KEYs integrity and confidentiality from the moment these are imported / generated on environment's HSM.

T.SigF_Misuse	Unauthorized use of the signature-function

This threat is about the tampering of security mechanisms related to the access to Signature creation function, the core of the problem is the fact an SCD signs something that the allowed signer doesn't meant to sign, this includes the ownership of an SCD and the SCD delegation.
To counter this threat the access to the Signature creation function is authorized by **OT.SigFunction_Usage** which controls the access based on authentication and authorization provided by **OT.Signatory_Auth**.
OT.Account_Separation also prevents the unauthorized inter-users access to SCD protection.
OT.Secure_Delegation ensure that SCD delegation and revoke procedures are performed in a secure way controlling that only authorized users can used SCD.
OT.Startup&Shutdown_Security also ensures that the access to Signature creation function is protected by the authentication modules and cannot be bypassed on initialization or shutdown time.
Another way an attacker can perform an unauthorized signature is to inject its own DTBS or DTBS/R in the invocation of the Signature creation function and/or either replaying stealed OTP VADs, those attacks are countered by securing the channels by which the sensible data travels and also having trusted SCAs. The trusted channels for the connections managed by vinCERTcore are enforced by **OT.Trusted_Comm** and are sufficiently strengthened by **OE.Configured**. Aditionally the trusted channel for the connection between vinCERTcore and RADIUS server is enforced by **OE.Secured_RADIUS**.
The **OE.Secure_SCA** ensures that this kind of tampers cannot be done in the SCA.
The **OE.Secure_Env** also ensures that the HSM cannot be used to favour this kind of tampers.
The **OE.Standard_Time_Source** guarantees that the authentication tokens are valid during the execution of the Signature creation function.

T.User_Impersonation	Unauthorized use of TOE functionality

This threat is about the tampering of security mechanisms related to the access to general functionality of the TOE. In this case the problem is that an attacker may use functions that belongs to a trusted user.
To counter this threat the access to the functionality of the TOE is authorized by **OT.Signatory_Auth** and **OT.Privileged_Auth** which performs the authentication of the users.
OT.Account_Separation prevents the unauthorized access to operatives not belonging to the users.
OT.Startup&Shutdown_Security ensures that the access to TOE functionalities is protected by the authentication modules before they are initialized and exposed on start-up and shutdown time.
The trusted channels for the authentication processes are protected by either **OT.Trusted_Comm** and **OE.Secured_RADIUS** so the credentials traveling within cannot be tampered, the trusted channel strength for the connections managed by vinCERTcore is assured by **OE.Configured**.
The **OE.Secure_Env** ensures that the external IT products cannot be used to perform this kind of tampers.
The **OE.Secure_SCA** ensures that this kind of tampers cannot be done in the SCA.
The **OE.Standard_Time_Source** guarantees that the authentication tokens are valid during the authentication procedure.

T.Sig_Forgery Misleading digital signature forgery

This threat addresses the threat of a verification of a digital signature by the SVD which does not detect the flaws on a misleading signature that's been forged without the SVD's paired SCD.
Diminishing the misleading signature forgery is done by applying a proper cryptographic configuration level for the TOE and this is assured by **OE.Configured** and **OE.Secure_HSM** for, respectively, making sure the TOE uses a strong cryptographic level for its operations and that this level is supported by the environment's HSM.

T.Config_Access Unauthorized modification of the TOE configuration

This threat talks about the unauthorized modification of the TOE configuration or wrong configurations that may lead to TOE malfunctions or security flaws.
To counter this thread the configuration is ciphered and can only be deciphered on TOE start-up thanks to **OT.Startup&Shutdown_Security**.
This cipher is correctly done and strong enough due to **OE.Certified_HSM**.
The access to the ciphering KEY and its password is protected by **OT.Key_Secure_Management** as well the generation and regeneration functions of these KEYs.
Only the authorized personnel can modify the configuration through TOE interfaces prior authentication thanks to **OT.Privileged_Auth** and the authorized personnel will not make configuration mistakes as stated on **OE.Competent_Users**.
Finally the configuration and security parameters as the KEY crypto strength and the algorithms used will be correct and strong enough as stated on **OE.Configured**.

T.Audit_Access Unauthorized access or generation denying of audit data

This threat deals with an unauthorized access to audit data or audit data generation function and either read it without permission, modify it, delete it, or denying its generation.
This threat is diminished by **OT.Startup&Shutdown_Security** by ensuring during the TOE startup the correct performance of the audit data generation function, it also ensures that no audit data is lost on shutdown.
OT.Privileged_Auth controls the authentication and access of privileged users to audit data related operations.
OT.Key_Secure_Management enforces the protection (use and access) of the KEY and its password used to generate the integrity of the audit data. It also protects the access to the management operatives related to the latter KEY to authorized users only.
Additionally **OE.Configured**, **OE.Secure_Env** and **OE.Certified_HSM** makes sure that the cryptographic configuration for the KEY and for the algorithm used in the generation of the audit data integrity protection are strong enough.
OT.Audit_Prot assures the audit exported data (audit archives) integrity.
OT.Trusted_Comm and **OE.Secure_Env** preserves the integrity of audit data when this one is exported from the TOE to the environment's database.
OE.Competent_Users ensures that users with authorized roles to access audit data won't perform any involuntary action that may jeopardize it.
OE.Audit_Review ensures the storage exhaustion for the TOE is never reached and therefore it does not represent a problem that may cause the audit data generation function to stop.

T.Audit_Archive Alteration of audit archive data

This threat is a problem about the modification of the data inside an exported audit archive. To mitigate this problem the exported archive will be shipped with integrity protection.
As this protection is generated by the TOE, **OT.Startup&Shutdown_Security** will ensure that the cryptographic parameters related to the archive generation will be correctly setup on the initialization of the TOE, those parameter will be strong enough thanks to **OE.Competent_Users** and **OE.Configured**.
The correct generation of the exported archive with such security is ensured by **OT.Audit_Prot** and can be achieved thanks to **OE.Certified_HSM**.

T.Backup_Archive	Alteration of backup data

This threat describes the attacks which try to alter the backup data, it is diminished by **OT.Privileged_Auth,** which controls the privileged user's access to backup data and backup operation; along with **OT.Backup_Prot** which preserves the backup data integrity and confidentiality.

In addition, **OE.Competent_Users** ensures that the privileged users responsible for backup operations are trained and won't perform any system damaging action towards it.

To diminish this treat **OE.Configured** and **OE.Certified_HSM** makes sure that the cryptographic level used to protect the integrity of backup data is strong enough.

4.3.2.2. OSPs and Security Objective Sufficiency

P.Crypto_Managment	Maintenance of the cryptography strength

This policy controls the procedures related to the maintenance of the cryptography strength.

The TOE cryptography strength is implemented in the start-up and in its operation by **OT.Startup&Shutdown_Security**, **OT.SCD_Secure_Lifecycle** and **OT.Key_Secure_Management**.

In order to enforce the policy, R.SecurityOfficer must be aware about the obsolescence and the vulnerabilities related to the cryptography (suitable algorithms and key lengths) used in the TOE configuration, enforced by **OE.Competent_Users**.

In order to update the security configuration, the R.SecurityOfficer must be authenticated in the TOE thanks to **OT.Privileged_Auth**.

The TOE also needs to be correctly configured and to work well with those levels of cryptography, enforced by **OE.Configured** and **OE.Certified_HSM**.

P.Standard_Time_Source	Maintenance of the standard time source

This policy is a service on which the TOE operating system relies for acquiring confinable time and date, many aspects of the TOE operations are using the system time which comes from this service.

OT.Startup&Shutdown_Security will enforce that in the initialization of the TOE the time from the operating system will be available in order to assure that it will be ready for the operations that use it.

OT.Signatory_Auth and **OT.Privileged_Auth** are heavy enforcing the use of the time from the operating system because on the authentication process a Time Stamped ticket is generated and the whole authentication mechanism is relying on that ticket.

The time from the operating system is used on auditing operatives to generate Time Stamps and for saving the time when the operations were made, the objectives **OT.Audit_Prot** and **OT.Backup_Prot** are enforcing those needs.

The Time Source from the TOE operating system must be configured and operated correctly to be trusted, this is enforced by **OE.Competent_Users** and **OE.Configured**. Additionally this Time Source must be a trustworthy service that is enforced by **OE.Secure_Env** and **OE.Standard_Time_Source**.

P.HSM_Backup	Management of HSM backups

This policy establishes mechanisms to make a safe copy (backup) of TOE's SCDs and KEYs.

OE.Competent_Users makes sure the backup procedure for the environment's HSM is done correctly by the operators. Additionally, **OE.Certified_HSM** and **OE.Secure_Env** ensures this one is trustworthy and reliable.

P.Audit_Review	Audit data reviewing

This policy establishes procedures for authorized auditor(s) to periodically review the audit data, analyse it, and respond properly to any security flaw or abnormal behaviour he may detect on the data.

OE.Audit_Review addresses the establishment of this organizational procedure for the audit data's reviewing by the authorized users. **OT.Startup&Shutdown_Security** ensures on TOE start-up that *Audit Module* is initialized correctly and audit data generation function is working properly. **OT.Audit_Prot** preserves de audit data integrity within the TOE and on the performance of the exportation functions, whenever this data is exported to the environment's database its integrity is protected by **OE.Secure_Env** addressing the reliability of the DB. **OT.Privileged_Auth** makes sure that only the authorized users are able to access audit data for its reviewing, additionally, **OE.Competent_Users** ensures that these users are trained and competent enough so they won't perform any harming to the data.

In order to work properly, the TOE itself and some environment IT products needs to have sufficient storage space as stated in **P.Storage_Review**. This is enforced by the correct reviewing and taking the necessary actions (i.e. adding additional storage media) on preventing storage exhaustion that is enforced by **OE.Competent_Users**.

P.Storage_Review	Storage status reviewing

This policy establishes procedures for the environment personnel to review the storage exhaustion status. **OE.Competent_Users** addresses the organization's personnel as the people responsible for the storage's free space control and delegates on them to take the measures necessary to ensure the TOE's correct functionality is not threatened by this cause.

4.3.2.3. Assumptions and Security Objective Sufficiency

A.Trained&Trusted establishes the trustworthiness of every TOE privileged role, including *R.Administrator*, *R.Operator*, *R.SecurityOfficer* and *R.Auditor*; and their preparation for operating the TOE. These user's trustworthiness and preparation addresses the **OE.Competent_Users** definition and ensures the establishment of **OE.Configured**'s specification which ensures the correct configuration for the TOE.

A.No_Malware establishes that there won't be any malware software installed on the same operating system as the TOE. This is addressed by **OT.Competent_Users** for ensuring that users operating the TOE won't install any unwanted software involuntarily, and by **OE.Secure_Env** which ensures the TOE's environment, in this case the same O.S. from which the TOE is running, does not have any malicious element installed on it that may try to perform actions against the TOE.

A.Configuration establishes that the TOE will be properly installed and configured according to product guides. This is addressed by **OE.Configured** which ensures that the TOE is actually installed and configured properly.

A.Trusted_IT_Products establishes the trustworthiness and reliability of the TOE's environment elements. This includes the environment's HSM, PKI *(vinCERTcamgr)*, Active Directory, RADIUS Authentication Server, Database, vinCERTagent, and vinCERTweb; those are addressed by either **OE.Secure_Env** and **OE.Secured_RADIUS**.

A.Trusted_SCA establishes that an R.Signer will use only a trustworthy SCA that creates and sends the DTBS or the DTBS/R the R.Signer wishes to sign in an appropriated form to be signed by the TOE. It is also implemented in compliance with functional requirements of CWA 14170.
This is directly addressed by **OE.Secure_SCA** which explicitly ensures that.

A.Trusted_Agents establishes the trustworthiness of external elements vinCERTagent and vinCERTweb, ensuring that these external elements won't perform any malicious action towards the TOE, this is addressed by **OE.Secure_Env**.

As stated in **A.Certified_HSM** the HSM will be hardware based, will meet the requirements identified in EN 419241 and/or will be a trustworthy system which is assured to EAL 4+ or higher in accordance to ISO/IEC 15408, or equivalent security criteria, or will meet the requirements identified in FIPS PUB 140-2 level 3 or higher. This is directly addressed by **OE.Certified_HSM** which explicitly ensures that.

A.No_Physical_Access establishes that no thread agents and users have direct physical access to the TOE. This is addressed by **OE.Secure_Env.**

4.4.Conclusion

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

5. Security requirements

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

Security functional requirements components given in section 6.1 *security functional requirements*

Operations for assignment, selection and refinement have been made. The TOE security assurance requirements statement given in section 6.2 "TOE Security Assurance Requirement" is drawn from the security assurance components from Common Criteria part 3 [3]. The following textual conventions are used in this chapter as part of every SFR:

- Iteration
  Allows a component to be used more than once with varying operations. A slash ("/") followed by an identifier placed at the end of the component indicates an iteration.
  In the case of a reference to an iteration or a group of the same iteration, the reference will be to the group of the iterations.
  For example, iterations FDP_ACF.1.1/Signer, FDP_ACF.1.2/Signer, FDP_ACF.1.3/Signer and FDP_ACF.1.4/Signer will be referred as FDP_ACF.1/Signer.

- Assignment
  Allows the specification of an identified parameter and it is represented in **bold.**

- Selection:
  Allows the specification of one or more elements from a list and it is represented in *italic*.

- Refinement:
  Allows the addition of details that are represented in **SMALL CAPITAL BOLD UNDERLINED.**

5.1. Security Functional Requirements

5.1.1. Security Audit (FAU)

5.1.1.1. Security audit automatic response (FAU_ARP)

5.1.1.1.1. Security alarms (FAU_ARP.1)

FAU_ARP.1.1

The TSF shall take **inform the involved user if exist, inform to configured list of warning event receivers, inform the authorised user and disable the associated policy that created the potential security violation** upon detection of a potential security violation.

Application note:
To perform the operation **inform to configured list of warning event,** Mail Server is used.

5.1.1.2. Security audit data generation (FAU_GEN)

5.1.1.2.1. Audit data generation (FAU_GEN.1)

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) **The events listed in Table 9: Audit events**.

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **none**.

Application note:
Follows a table of all auditable events:

Event	Description
Start-up	Start-up of the TOE
Shut-down	Shutdown of the TOE
Login	Login operation (First and second factor authentication operations) and authentication failures, retries and potential security violations in case of massive login attempts
Import certificate	Import of software certificate from vinCERTweb
Request certificate	Request of new certificate and the creation of its associated key-pair
Enroll certificate	Enroll of certificate
Delete certificate	Deletion of certificate and its associated key-pair
Signature creation	Secure signature creation
Data Decryption	Secure data decryption
Key Activation	Key derivation for cryptographic operations
Qualified delegation	Delegate signature capability to another Signer
Accept delegation	Accept signature delegation capability.
Revoke delegation	Revoke signature delegation capability.
Advanced delegation	Delegate signature capability to another signer.
Generate backup	Generation of backup archive
Restore system	Restore backup archive
Configure system	Configure environment or security parameters.
Generate audit archive	Generation of audit archive

Event	Description
Review audit	Audit data review
Regenerate keys	Regenerate infrastructure and control keys
Audit verification	Verify audit integrity
Audit purge	Deletion of audit blocks stored in audit archive
Logout	System session locking mechanism or user forced logout
Console disconnected	Console session is closed by inactivity
Modify policy	Policy is modified by user
Trusted path channel	Trusted path failure
Potential key violation	Potential key violation is detected
Send alert	An alert email is sent when potential security violation is detected

Table 9: Audit events

5.1.1.2.2. User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.3. Security audit analysis (FAU_SAA)

5.1.1.3.1. Potential violation analysis (FAU_SAA.1)

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events: Accumulation or combination of **authentication failed events or enabling policy for signing failed in determined configurable time interval** known to indicate a potential security violation;
b) **None**.

5.1.1.4. Security audit review (FAU_SAR)

5.1.1.4.1. Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **user accounts with role R.Audit** with the capability to read **all** from the audit records.

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

5.1.1.4.2. Restricted audit review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

5.1.1.4.3. Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply **selection with a subset of the following attributes:**

- **before date,**
- **after date**
- **userID**
- **event type**
- **certificate**

and ordered by audit identificator of audit data based on **the following relation:**

Search audit entries that entry.date < before date, entry.date > after date, entry.UserID = UserID, entry.eventType = event type, entry.certificate = certificate, ordered by one of the criteria.

5.1.1.5. Security audit event storage (FAU_STG)

5.1.1.5.1. Guarantees of audit data availability (FAU_STG.2)

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

FAU_STG.2.2 The TSF shall be able to *detect* unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that **all** stored audit records will be maintained when the following conditions occur: *audit storage exhaustion, failure.*

5.1.2. Cryptographic support (FCS)

5.1.2.1. Cryptographic key management (FCS_CKM)

5.1.2.1.1. Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **zeroization** that meets the following: [8]

Application note:
Zeroization is applied to a generated SAD after a key creation or activation. This operation is performed within TOE.

5.1.2.2. Cryptographic operation (FCS_COP)

5.1.2.2.1. Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform **Key Derivation** in accordance with a specified cryptographic algorithm **PBKDF2** and cryptographic key sizes **2048 bit** that meet the following: [9] **.**

Application note:
Key Derivation is performed within TOE.

5.1.3. User data protection (FDP)

5.1.3.1. Access Control Policy (FDP_ACC)

The following table is a summary of the next Operations.

Subject	Operation	Object
Privileged user Signer user	First factor authentication	TOE instance User Repository Connection Data Configuration User Account
Privileged user Signer user	Second factor authentication	TOE instance User Repository Connection Data Configuration User Account
Privileged user	Generate backup	TOE instance User Account Configuration
Privileged user	Restore system	TOE instance User Account Backup archive
Privileged user	Operations defined in *FMT_SMF.1:* Start up Shut down	TOE instance User Account
Privileged user	Configure environment	TOE instance User Account Configuration
Privileged user	Regenerate internal keys applied to database key	TOE instance User Account Configuration Database
Privileged user	Regenerate internal keys applied to other infrastructure and control keys	TOE instance User Account Configuration
Privileged user	Audit purge	TOE instance User Account Audit end block
Privileged user	Configure security	TOE instance User Account Configuration
Privileged user	Audit review	User Account TOE instance Audit records
Privileged user	Audit verify	User Account TOE instance Audit records
Privileged user	Generate audit archive	User Account TOE instance Audit records
Signer user	Certificate import	User Account TOE instance SCD/SVD pair
Signer user	Certificate request	User Account TOE instance
Signer user	Certificate enroll	User Account TOE instance PKI request SCDid/SVD pair

Subject	Operation	Object
Signer user Privileged user	Certificate delete	User Account TOE instance Certificate Light Policy Strong Policy SCDid/SVD pair
Signer user	Renovate advanced certificate	User Account TOE instance Certificate Light Policy
Signer user	Renovate qualified certificate	User Account TOE instance Certificate Strong Policy SCDid/SVD pair
Signer user Privileged user	Policy edition	User Account TOE instance Certificate Light Policy Strong Policy
Signer user	Light policy delete	User Account TOE instance Certificate Light Policy
Signer user	Certificate change pin	User Account TOE instance Certificate Light Policy Strong Policy SCDid/SVD pair
Signer user	Delegate advanced signature	User Account TOE instance Certificate Light Policy
Signer user	Delegate qualified signature	User Account TOE instance Certificate Strong Policy SCDid/SVD pair
Signer user	Revoke qualified delegation	User Account TOE instance Certificate Strong Policy
Signer user	Accept delegation	User Account TOE instance Certificate Light Policy Strong Policy
Signer user	Signature creation	User Account TOE instance Light Policy Strong Policy Static VAD DTBS/R

Table 10: Access control policy summary

5.1.3.1.1. Subset access control (FDP_ACC.1)

FDP_ACC.1.1/Management

The TSF shall enforce the **Management User Access Control Policy SFP** on

Subject:

- **Privileged user**

Operations:

- **First factor authentication**
- **Second factor authentication**
- **Generate backup**
- **Restore system**
- **Operations defined in *FMT_SMF.1***
    - **Start up**
    - **Shut down**
- **Configure environment**
- **Regenerate internal keys**
    - **Database key**
    - **Other infrastructure and control keys (Ticket Key, Configuration Key and Audit Key)**
- **Audit purge**
- **Configure security**
- **Audit review**
- **Audit verify**
- **Generate audit archive**
- **Certificate delete**
- **Policy edition**

Objects:

- **TOE instance**
- **User Repository Connection Data**
- **Configuration**
- **User Account**
- **Backup archive**
- **Database**
- **Audit end block**
- **Audit records**
- **Certificate**
- **Light Policy**
- **Strong Policy**

FDP_ACC.1.1/Signer

The TSF shall enforce the **Signer User Access Control Policy SFP** on

Subject:

- **Signer user**

Operations:

- **First factor authentication**
- **Second factor authentication**
- **Certificate import**
- **Certificate request**
- **Certificate enroll**
- **Certificate delete**
- **Renovate advanced certificate**
- **Renovate qualified certificate**
- **Policy edition**
- **Light policy delete**
- **Certificate change pin**
- **Delegate advanced signature**
- **Delegate qualified signature**
- **Revoke qualified delegation**
- **Accept delegation**
- **Signature creation**

Objects:

- **TOE instance**
- **User Repository Connection Data**
- **Configuration**
- **User Account**
- **SCD/SVD pair**
- **PKI request**
- **SCDid/SVD pair**
- **Light Policy**
- **Strong Policy**
- **Certificate**
- **Static VAD**
- **DTBS/R**

5.1.3.2. Access Control Functions (FDP_ACF)

5.1.3.2.1. Security attribute based access control (FDP_ACF.1)

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

Subject	Attribute	Status
Privileged user attributes		
Privileged user	Role	R.Administrator, R.Operator, R.Auditor, R.SecurityOfficer
Privileged user	Status	Locked, unlocked, enabled, disabled
Privileged user	UUID	Value, empty
Signer user attributes		
Signer user	Role	R.CertOwner, R.Signer
Signer user	Status	Locked, unlocked, enabled, disabled
Signer user	UUID	Value, empty

Table 11: Subject security attributes

Object	Attribute	Status
TOE Instance general attributes		
TOE Instance	Mode	Management, Operative
User repository connection data attributes		
User repository connection data	Configuration connection parameters	Management, Operative
Configuration attributes		
Configuration	Integrity	Yes, no
Configuration	AD connection data	Value, empty
Configuration	Radius connection data	Value, empty
User Account attributes		
User Account	UUID	Value, empty
User Account	AD validation status	Valid, invalid
User Account	OTP validation status	Valid, invalid
User Account	Static password AD Note: The value is not kept as part of the user account	Value, empty
User Account	OTP VAD Note: The value is not kept as part of the user account	Value, empty
User Account	Static VAD Note: The value is not kept as part of the user account	Value, empty
Backup archive general attributes		
Backup archive	Integrity	Yes, no
Backup archive	Confidentiality	Yes, no
Database attributes		
Database	Integrity	Yes, no
Audit end block attributes		
Audit end block	Block number	Value, empty
Audit records attributes		
Audit records	Record number	Value, empty
SCD/SVD pair attributes		
SCD/SVD pair	SCD	Value, empty
PKI request attributes		
PKI request	UUID	Value, empty
PKI request	Status	ENROLL, ISSUED, ERROR
SCDid/SVD pair attributes		
SCDid/SVD pair	SCD	Value, empty

Policy general attributes		
Policy	idUser UUID	Value, empty
Policy	Integrity	Yes, no
Policy	Type	Light, Strong
Policy	Enabled	Yes, no
Policy	Certificate ID	Value, empty
Light Policy attributes		
Light Policy	Mode	Ownership, Signatory
Light policy	VAD Protection enabled	Yes, no
Light policy	VAD/R	Value, empty
Strong Policy attributes		
Strong policy	Delegation status	None, transfer, delegated
Strong policy	Strong SCDid	Value, empty
Certificate attributes		
Certificate	ID	Value, empty
Certificate	IdOwner UUID	Value, empty
Static VAD attributes		
Static VAD	VAD/R	Value, empty
DTBS/R attributes		
DTBS/R	Size	Value, empty

Table 12: Object security attributes

FDP_ACF.1.1/Management

The TSF shall enforce the **Management User Access Control Policy SFP** to objects based on the following:

Subject Attributes:

- **Privileged user**

Object Attributes:

- **TOE instance attributes**
- **User Repository Connection Data attributes**
- **Configuration attributes**
- **User Account attributes**
- **Backup archive attributes**
- **Database attributes**
- **Audit end block attributes**
- **Audit records attributes**

FDP_ACF.1.2/Management

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:
For operation First factor authentication:
All the following conditions are needed (AND):

- **TOE instance connection data corresponds to User repository connection data**
- **User repository connection data is generated with configuration connection parameters**
- **User Account Static password AD = Value**

For operation Second factor authentication all the following conditions are needed (AND):

- **Privileged User Role = R.Administrator, R.Operator, R.Auditor or R.SecurityOfficer**
- **TOE instance connection data corresponds to User repository connection data**
- **User repository connection data is generated with configuration connection parameters**
- **User Account AD validation status = yes**
- **User Account OTP validation status = no**
- **User Account OTP VAD = Value**

For operation Generate backup all the following conditions are needed (AND):

- **Privileged user Status = Enabled**
- **Privileged user UUID = User Account UUID**
- **TOE instance Mode = Management**
- **User Account AD validation status = Valid**

One of the following conditions are needed (OR):

- **Privileged User Role = R.Administrator**
- **Privileged User Role = R.Operator**

For operation Restore system all the following conditions are needed (AND):

- **Privileged user Status = Enabled**
- **Privileged user UUID = User Account UUID**
- **TOE instance Mode = Management**
- **User Account AD validation status = Valid**
- **Backup archive Integrity = Yes**
- **Backup archive Confidentiality =Yes**

One of the following conditions are needed (OR):

- **Privileged User Role = R.Administrator**
- **Privileged User Role = R.Operator**

For operations defined in FMT_SMF.1: Start up and shut down, all the following conditions are needed (AND):

- **Privileged user Status = Enabled**
- **Privileged user UUID = User Account UUID**
- **User Account AD validation status = Valid**

One of the following conditions are needed (OR):

- **TOE instance Mode = Management**
- **TOE instance Mode = Operative**

One of the following conditions are needed (OR):

- **Privileged User Role = R.Administrator**
- **Privileged User Role = R.Operator**

For operation Configure environment all the following conditions are needed (AND):

- **Privileged user Role = R.Administrator**
- **Privileged user Status = Enabled**
- **Privileged user UUID = User Account UUID**
- **TOE instance Mode = Management**
- **User Account AD validation status = Yes**

For the operation Regenerate internal keys applied to database key all the following conditions are needed (AND):

- **Privileged user Role = R.Administrator**
- **Privileged user Status = Enabled**
- **Privileged user UUID = User Account UUID**
- **TOE instance Mode = Management**
- **User Account AD validation status = Yes**
- **Database Integrity = Yes**

For operation Regenerate internal keys applied to other infrastructure and control keys all the following conditions are needed (AND):

- **Privileged user Role = R.Administrator**
- **Privileged user Status = Enabled**
- **Privileged user UUID = User Account UUID**
- **TOE instance Mode = Management**
- **User Account AD validation status = Yes**

For operation Audit purge all the following conditions are needed (AND):

- **Privileged user Role = R.Administrator**
- **Privileged user Status = Enabled**
- **Privileged user UUID = User Account UUID**
- **User Account AD validation status = Yes**
- **Audit end block Block number = Value**

One of the following conditions are needed (OR):

- **TOE instance Mode = Management**
- **TOE instance Mode = Operative**

For operation Configure security all the following conditions are needed (AND):

- **Privileged user Role = R.SecurityOfficer**
- **Privileged user Status = Enabled**
- **Privileged user UUID = User Account UUID**
- **TOE instance Mode = Management**
- **User Account AD validation status = Yes**

For operation Audit review all the following conditions are needed (AND):

- Privileged user Role = R.Auditor
- Privileged user Status = Enabled
- Privileged user UUID = User Account UUID
- User Account AD validation status = Yes
- Audit records Record number = Value

One of the following conditions are needed (OR):

- TOE instance Mode = Management
- TOE instance Mode = Operative

For operation Audit verify all the following conditions are needed (AND):

- Privileged user Role = R.Auditor
- Privileged user Status = Enabled
- Privileged user UUID = User Account UUID
- User Account AD validation status = Yes
- Audit records Record number = Value

One of the following conditions are needed (OR):

- TOE instance Mode = Management
- TOE instance Mode = Operative

For operation Generate audit archive all the following conditions are needed (AND):

- Privileged user Role = R.Auditor
- Privileged user Status = Enabled
- Privileged user UUID = User Account UUID
- User Account AD validation status = Yes
- Audit records Record number = Value

One of the following conditions are needed (OR):

- TOE instance Mode = Management
- TOE instance Mode = Operative

For operation Certificate delete all the following conditions are needed (AND):

- Privileged user Role = R.Administrator
- Privileged user Status = Enabled
- Privileged user UUID = User Account UUID
- TOE instance Mode = Operative
- User Account AD validation status = Valid
- User Account OTP validation status = Valid
- Certificate ID = Value
- Policy Integrity = Yes

For operation Policy edition, all the following conditions are needed (AND):

- Privileged user Role = R.Administrator or R.Operator
- Privileged user Status = Enabled
- Privileged user UUID = User Account UUID
- TOE instance Mode = Operative
- User Account AD validation status = Valid
- User Account OTP validation status = Valid
- Certificate ID = Value
- Policy Integrity = Yes

If Policy Type = Strong (OR):

- Strong Policy Status = None
- Strong Policy Status = Delegated

FDP_ACF.1.3/Management

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

FDP_ACF.1.4/Management

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

FDP_ACF.1.1/Signer

The TSF shall enforce the **Signer User Access Control Policy SFP** to objects based on the following:

Subject Attributes:

- **Signer user**

Object Attributes:

- **TOE instance attributes**
- **User Repository Connection Data attributes**
- **Configuration attributes**
- **User Account attributes**
- **Light Policy (policy general attributes included) attributes**
- **Strong Policy (policy general attributes included) attributes**
- **PKI request attributes**
- **SCDid/SVD pair attributes**
- **Light Policy attributes (Policy general attributes included)**
- **Strong Policy attributes (Policy general attributes included)**
- **Certificate attributes**
- **Static VAD attributes**
- **DTBS/R attributes**

FDP_ACF.1.2/Signer

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

For operation First factor authentication:
All the following conditions are needed (AND):

- **TOE instance connection data corresponds to User repository connection data**
- **User repository connection data is generated with configuration connection parameters**
- **User Account Static password AD = Value**

For operation Second factor authentication:
All the following conditions are needed (AND):

- **Signer user Role = R.CertOwner or R.Signer**
- **TOE instance connection data corresponds to User repository connection data**
- **User repository connection data is generated with configuration connection parameters**
- **User Account AD validation status = yes**
- **User Account OTP validation status = no**
- **User Account OTP VAD = Value**

For operation Certificate import, all the following conditions are needed (AND):

- **Signer user Role = R.CertOwner**
- **Signer user Status = Enabled**

- Signer user UUID = User Account UUID
- TOE instance Mode = Operative
- User Account AD validation status = Valid
- User Account OTP validation status = Valid
- SCD/SVD pair SCD = Value

For operation Certificate request, all the following conditions are needed (AND):

- Signer user Role = R.CertOwner
- Signer user Status = Enabled
- Signer user UUID = User Account UUID
- TOE instance Mode = Operative
- User Account AD validation status = Valid
- User Account OTP validation status = Valid

For the operation Certificate Enroll all the following conditions are needed (AND):

- Signer user Role = R.CertOwner
- Signer user Status = Enabled
- Signer user UUID = User Account UUID
- TOE instance Mode = Operative
- User Account AD validation status = Valid
- User Account OTP validation status = Valid
- PKI request UUID = Signer user UUID
- PKI request Status = ENROLL
- SCDid/SVD pair SCD = Value

For operation Certificate delete all the following conditions are needed (AND):

- Signer user Role = R.CertOwner
- Signer user Status = Enabled
- Signer user UUID = User Account UUID
- TOE instance Mode = Operative
- User Account AD validation status = Valid
- User Account OTP validation status = Valid
- Certificate ID = Value
- Certificate IdOwner UUID = Signer user UUID
- Policy Integrity = Yes

One of the following conditions are needed (OR):

- Policy Type = Light
- Policy Type = Strong

If Policy Type = Light (AND):

- Light Policy Mode = Ownership

If Policy Type = Strong (AND):

- Strong Policy Delegation Status = None
- SCDid/SVD pair SCD = Value

For operation Renovate advanced certificate, all the following conditions are needed (AND):

- Signer user Role = R.CertOwner
- Signer user Status = Enabled
- Signer user UUID = User Account UUID
- TOE instance Mode = Operative
- User Account AD validation status = Valid
- User Account OTP validation status = Valid
- Certificate ID = Value
- Certificate IdOwner UUID = Signer user UUID
- Policy Type = Light

- **Policy Integrity = Yes**
- **Light Policy Mode = Ownership**

For operation Renovate qualified certificate, all the following conditions are needed (AND):

- **Signer user Role = R.CertOwner**
- **Signer user Status = Enabled**
- **Signer user UUID = User Account UUID**
- **TOE instance Mode = Operative**
- **User Account AD validation status = Valid**
- **User Account OTP validation status = Valid**
- **Certificate ID = Value**
- **Certificate IdOwner UUID = Signer user UUID**
- **Policy Type = Strong**
- **Policy Integrity = Yes**
- **SCDid/SVD pair SCD = Value**

For operation Policy edition, all the following conditions are needed (AND):

- **Signer user Role = R.CertOwner**
- **Signer user Status = Enabled**
- **Signer user UUID = User Account UUID**
- **TOE instance Mode = Operative**
- **User Account AD validation status = Valid**
- **User Account OTP validation status = Valid**
- **Certificate ID = Value**
- **Policy idUser UUID = Signer user UUID**
- **Policy Integrity = Yes**
- **Certificate IdOwner UUID = Signer user UUID**

If Policy Type = Strong (OR):

- **Strong Policy Status = None**
- **Strong Policy Status = Delegated**

For operation Light policy delete, all the following conditions are needed (AND):

- **Signer user Role = R.CertOwner**
- **Signer user Status = Enabled**
- **Signer user UUID = User Account UUID**
- **TOE instance Mode = Operative**
- **User Account AD validation status = Valid**
- **User Account OTP validation status = Valid**
- **Certificate ID = Value**
- **Policy Type = Light**
- **Policy idUser UUID = Signer user UUID**
- **Certificate IdOwner UUID = Signer user UUID**

For operation Certificate change pin, all the following conditions are needed (AND):

- **Signer user Status = Enabled**
- **Signer user UUID = User Account UUID**
- **TOE instance Mode = Operative**
- **User Account AD validation status = Valid**
- **User Account OTP validation status = Valid**
- **Certificate ID = Value**
- **Policy idUser UUID = Signer user UUID**
- **Policy Integrity = Yes**

One of the following conditions are needed (OR):

- **Signer user Role = R.Signer**
- **Signer user Role = R.CertOwner**

If Policy Type = Strong (AND):

- **SCDid/SVD pair SCD = Value**

For operation Delegate advanced signature, all the following conditions are needed (AND):

- **Signer user Role = R.CertOwner**
- **Signer user Status = Enabled**
- **Signer user UUID = User Account UUID**
- **TOE instance Mode = Operative**
- **User Account AD validation status = Valid**
- **User Account OTP validation status = Valid**
- **Certificate ID = Value**
- **Certificate IdOwner UUID = Signer user UUID**
- **Policy Type = Light**
- **Policy Integrity = Yes**
- **Light Policy Mode = Ownership**

For operation Delegate qualified signature, all the following conditions are needed (AND):

- **Signer user Role = R.CertOwner**
- **Signer user Status = Enabled**
- **Signer user UUID = User Account UUID**
- **TOE instance Mode = Operative**
- **User Account AD validation status = Valid**
- **User Account OTP validation status = Valid**
- **Certificate ID = Value**
- **Policy idUser UUID = Signer user UUID**
- **Policy Type = Strong**
- **Policy Integrity = Yes**
- **Strong policy Delegation status = None**
- **SCDid/SVD pair SCD = Value**

For operation Revoke qualified delegation, all the following conditions are needed (AND):

- **Signer user Role = R.CertOwner**
- **Signer user Status = Enabled**
- **Signer user UUID = User Account UUID**
- **TOE instance Mode = Operative**
- **User Account AD validation status = Valid**
- **User Account OTP validation status = Valid**
- **Certificate ID = Value**
- **Certificate IdOwner UUID = Signer user UUID**
- **Policy Type = Strong**
- **Policy Integrity = Yes**

One of the following conditions are needed (OR):

- **Strong policy Delegation status = Transfer**
- **Strong policy Delegation status = Delegated**

For operation Accept delegation all the following conditions are needed (AND):

- **Signer user Status = Enabled**
- **Signer user UUID = User Account UUID**
- **TOE instance Mode = Operative**
- **User Account AD validation status = Valid**
- **User Account OTP validation status = Valid**

- **Certificate ID = Value**
- **Policy Type = Strong**
- **Policy Integrity = Yes**
- **Strong policy Delegation status = Transfer**

One of the following conditions are needed (OR):

- **Signer user Role = R.Signer**
- **Signer user Role = R.CertOwner**

For Signature creation operation all the following conditions are needed (AND):

- **Signer user Status = Enabled**
- **Signer user UUID = User Account UUID**
- **TOE instance Mode = Operative**
- **User Account AD validation status = Valid**
- **User Account OTP validation status = Valid**
- **Policy idUser UUID = Signer user UUID**
- **Policy Integrity = Yes**
- **Policy Enabled = Yes**
- **DTBS/R Size = Value**

One of the following conditions are needed (OR):

- **Signer user Role = R.Signer**
- **Signer user Role = R.CertOwner**

One of the following conditions are needed (OR):

- **Policy Type = Light**
- **Policy Type = Strong**

Additionally, one of the following set of rules must be applied:

I – Signing with Light policy without VAD protection:

- **Light Policy VAD protection enabled = No**

II – Signing with Light policy with VAD protection:

- **Light Policy VAD Protection enabled = Yes**
- **Static VAD VAD/R = Light Policy VAD/R**

III – Signing with Strong policy:

- **Strong Policy Delegation status = None or Delegated**
- **User Account Static VAD can activate Strong Policy SCDid**
- **Strong Policy SCDid is correlated to Signer user UUID**

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

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

5.1.3.3. Export from the TOE (FDP_ETC)

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

FDP_ETC.1.1 The TSF shall enforce the **Management User Access Control Policy SFP, Signer User Access Control Policy SFP** when exporting user data, controlled under the SFP(s), outside of the TOE.

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

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

FDP_ETC.2.1 The TSF shall enforce the **Management User Access Control Policy SFP, Signer User Access Control Policy SFP** when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE:

- **In export archive operation: Archive is signed and verified**.
- **In review audit operation: Audit entries are correctly signed**
- **In generate backup operation**: **Backup data is encrypted and signed**
- **In policy management: policy have correct integrity**

5.1.3.4. Import from outside of the TOE (FDP_ITC)

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

FDP_ITC.1.1 The TSF shall enforce the **Management User Access Control Policy SFP, Signer User Access Control Policy SFP** 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: **none**

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

FDP_ITC.2.1 The TSF shall enforce the **Management User Access Control Policy SFP, Signer User Access Control Policy SFP** 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:

- **The policies have a correct integrity data**.
- **The audit entries have a correct integrity data**.
- **The backup archive have a correct integrity and confidentiality data**.
- **For signature creation function, the signed data is verified with its corresponding SVD.**

5.1.3.5. Residual Information Protection (FDP_RIP)

5.1.3.5.1. Subset residual information protection (FDP_RIP.1)

FDP_RIP.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*deallocation of the resource from*] the following objects: **SCDid/SVD pair.SCD handler, Signer.Static VAD, Signer.OTP VAD, User Account.Static password AD, SCD/SVD pair, KEY id, KEY password**.

5.1.3.6. Rollback (FDP_ROL)

5.1.3.6.1. Basic rollback (FDP_ROL.1)

FDP_ROL.1.1 The TSF shall enforce **Management User Access Control Policy SFP** to permit the rollback of the **saved system status** on the **configuration data**.

FDP_ROL.1.2 The TSF shall permit operations to be rolled back within the **none**.

5.1.3.7. Stored Data Integrity (FDP_SDI)

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

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for **integrity errors** on all objects, based on the following attributes: **Policy.Integrity**.

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall **discard current operation and send warning message**.

5.1.3.8. Inter-TSF user data integrity transfer protection (FDP_UIT)

5.1.3.8.1. Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1/Backup-archive The TSF shall enforce the **Management User Access Control Policy SFP** to *receive* user data in a manner protected from *modification* errors.

FDP_UIT.1.2/Backup-archive The TSF shall be able to determine on receipt of user data, whether *modification* has occurred.

FDP_UIT.1.1/Audit-archive The TSF shall enforce the **Management User Access Control Policy SFP** to *transmit* user data in a manner protected from *modification* errors.

FDP_UIT.1.2/Audit-archive The TSF shall be able to determine on receipt of user data, whether *modification* has occurred.

5.1.4. Identification and authentication (FIA)

5.1.4.1. Authentication Failure (FIA_AFL)

5.1.4.1.1. Authentication failure handling (FIA_AFL.1)

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

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

- **For 1st factor login, notify user (And disconnect console session if the login was attempted from admin console).**
- **For 2nd factor login, cancel authentication session and notify user.**
- **For SCD Activation, disable the SCD key for signature.**

Application note:
Although the TSF requires that user is authenticated, the authentication process is delegated to the operational environment.

5.1.4.1. User attribute definition (FIA_ATD)

5.1.4.1.1. User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **UID, UUID, Status, Role, AD validation status, OTP validation status, Mail, Name, Full name.**

Application note:
The following table describes the user attributes:

User account attributes	Description	Values
UID	User identifier.	Value, empty
UUID	User unique identifier	Value, empty
Status	User status	Enabled/disabled and Unblocked/blocked
Role	User role	R.CertOwner, R.Signer, R.Administrator, R.Operator, R.Auditor, R.SecurityOfficer
AD validation status	User authentication status in active directory	Yes, no
OTP validation status	User authentication status in radius server	Yes, no
Mail	User mail	Value, empty
Name	User name	Value, empty
Full name	User complete name	Value, empty

Table 13: TOE user attributes

5.1.4.2. User Authentication (FIA_UAU)

5.1.4.2.1. Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow **establishing a trusted path** on behalf of the user to be performed before the user is authenticated.

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

Application note:
Although the TSF requires that user is authenticated, the authentication process is delegated to the operational environment.

5.1.4.2.2. Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide

- **Static user password authentication**
- **OTP dynamic user password**

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **if (Subject) User_Account.Role = R.Signer or R.CertOwner multiple authentication is mandatory for digital signature operation, SCD generation and SCD revocation. For console related operations multiple authentication is not required.**

Application note:
Although the TSF requires that user is authenticated, the authentication process is delegated to the operational environment.

5.1.4.2.3. Re-authenticating (FIA_UAU.6)

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **Re-authentication SHALL be mandatory after log out**.

Application note:
Although the TSF requires that user is authenticated, the authentication process is delegated to the operational environment.

5.1.4.3. User identification (FIA_UID)

5.1.4.3.1. Timing of identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow **Establishing a trusted path between remote user and the TOE** on behalf of the user to be performed before the user is identified.

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

Application note:
Any attempt to perform a TSF related request without being authenticated previously will reject the attempt having a dedicated entry in the audit log.

Application note:
Although the TSF requires that user is identified, the identification process is delegated to the operational environment.

5.1.4.1. User-subject binding (FIA_USB)

5.1.4.1.1. User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **UID** and **UUID**.

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

- **UID to sAMAccountName from AD**
- **UUID to SID from AD**

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **none**.

5.1.5. Security management (FMT)

5.1.5.1. Management of functions in TSF (FMT_MOF)

5.1.5.1.1. Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to *enable* the functions **described in the following table** to **roles mapped in the following table**.

Application note:
The following table lists de correlation of TOE administrative functions based on roles:

Functions/Roles	Administrator functions	Operator functions	Security Officer functions	Auditor functions
Generate backup	X	X		
Restore system	X	X		
Start up	X	X		
Shut down	X	X		
Configure environment	X			
Regenerate internal keys	X			
Audit purge	X			
Configure security			X	
Audit review				X
Audit verify				X
Generate audit archive				X

Table 14: Function/Role mapping

5.1.5.2. Management of security attributes (FMT_MSA)

5.1.5.2.1. Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1/Key-Regen The TSF shall enforce the **Management User Access Control Policy SFP** to restrict the ability to *modify* the security attributes **Integrity from Policy registers** to **R.Administrator**.

FMT_MSA.1.1/Signatory The TSF shall enforce the **Signer User Access Control Policy SFP** to restrict the ability to *query, modify, delete, create and use to sign* the security attributes **SCDid, Light policy security attributes and Strong policy security attributes** to **R.CertOwner or R.Signer**.

5.1.5.2.2. Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **Management User Access Control Policy SFP, Signer User Access Control Policy SFP** to provide *restrictive* default values for security attributes that are used to enforce the SFP.

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

5.1.5.3. Specification of Management Function (FMT_SMF)

5.1.5.3.1. Specification of Management Functions (FMT_SMF.1)

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

- **Generate backup**
- **Restore system**
- **Start-up the TOE**
- **Shut-down the TOE**
- **Configure environment**
- **Regenerate Internal Keys**
- **Audit purge**
- **Configure security**
- **Review audit records**
- **Verify audit trail**
- **Generate audit archive**

5.1.5.4. Security management roles (FMT_SMR)

5.1.5.4.1. Security roles (FMT_SMR.2)

FMT_SMR.2.1 The TSF shall maintain the roles **R.Administrator, R.CertOwner, R.Auditor, R.Signer, R.Operator, and R.SecurityOfficer**.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions
A user SHOULD NOT be authorized to take on more than one of roles R.SecurityOfficer, R.Administrator, R.Operator, R.Auditor, R.CertOwner and R.Signer;
AND
A user authorized to assume a R.SecurityOfficer role is not authorized to assume a R.Auditor role;
AND
A user authorized to assume an R.Administrator role and/or an R.Operator role is not authorized to assume an R.Auditor role and/or an R.SecurityOfficer role are satisfied.

5.1.6. Protection of the TSF (FPT)

5.1.6.1. Inter-TSF TSF Data Consistency (FPT_TDC)

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

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret:

- **Audit entries**
- **Backup data**
- **Policy registry**
- **Signed data**
- **Configuration**

when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use:

- **Data integrity of audit entry**
- **Data integrity and the confidentiality of backup data**
- **Data integrity of policy**
- **Signed data verification**
- **Configuration integrity and confidentiality**

when interpreting the TSF data from another trusted IT product.

5.1.6.2. TSF self-test (FPT_TST)

5.1.6.2.1. TSF testing (FPT_TST.1)

FPT_TST.1.1 The TSF shall run a suite of self tests *during initial start-up* to demonstrate the correct operation of *the TSF*.

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of ***TSF data***.

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of ***TSF executable code***.

5.1.7. TOE access (FTA)

5.1.7.1. Session locking and termination (FTA_SSL)

5.1.7.1.1. TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive session after *an administrator configurable positive integer within **30-600 seconds***.

5.1.7.1.2. User-initiated termination (FTA_SSL.4)

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

5.1.7.2. TOE session establishment (FTA_TSE)

5.1.7.2.1. TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **incoming connections from the external IT products vinCERTagent, vinCERTweb and SSH client not using SSL/TLS protocol.**

5.1.8. Trusted path/channels (FTP)

5.1.8.1. Inter-TSF trusted channel (FTP_ITC)

5.1.8.1.1. Inter-TSF trusted channel (FTP_ITC.1)

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 *the TSF* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

- **User Account Credential (static password) Validation and User Account recovery in AD-Server communication**.
- **SCD/SVD creation, SCD/SVD activation, Signature creation, Signature verification, Cipher data, Decipher data, SCD/SVD deactivation, SCD/SVD delete, SVD recovery, SCD/SVD correspondence verification, SYM-KEY creation, SYM-KEY activation, SYM-KEY signature creation, SYM-KEY signature verification in HSM communication**
- **Certificate Request and Enroll Certificate in vinCERTcamgr communication**
- **Data get, Data update, Data delete and Data insert in database communication**
- **Send notifications in SMTPServer communication**

5.1.8.2. Trusted path (FTP_TRP)

5.1.8.2.1. Trusted path (FTP_TRP.1)

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

FTP_TRP.1.2 The TSF shall permit *the TSF and remote users* to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *initial user authentication, TSF communication with external trusted IT products*.

5.2. Security Assurance Requirements

The assurance level for this TOE is EAL4+ ALC_FLR.2

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

Table 15: Assurance requirements for EAL4+ ALC_FLR.2

Follows a SFR dependency satisfaction table:

Requirement	Dependences
FAU_ARP.1	FAU_SAA.1
FAU_GEN.1	FPT_STM.1 Satisfied dependence: FPT_STM.1 is not required because the TOE relies on the system time to timestamp audit events and it is assumed (A.Configuration, A.Trusted_IT_Products, A.No_Physical_Access, A.No_Malware, OE.Secure_Env, and OE.Standard_Time_Source) that this time is reliable.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1
FAU_SAA.1	FAU_GEN.1
FAU_SAR.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1
FAU_STG.2	FAU_GEN.1
FCS_CKM.4	FDP_ITC.1
FCS_COP.1	FDP_ITC.1 FCS_CKM.4
FDP_ACC.1/Management	FDP_ACF.1/Management
FDP_ACF.1/Management	FDP_ACC.1/Management FMT_MSA.3
FDP_ACC.1/Signer	FDP_ACF.1/Signer
FDP_ACF.1/Signer	FDP_ACC.1/Signer FMT_MSA.3
FDP_ETC.1	FDP_ACC.1
FDP_ETC.2	FDP_ACC.1
FDP_ITC.1	FDP_ACC.1 FMT_MSA.3
FDP_ITC.2	FDP_ACC.1 FTP_ITC.1 FPT_TDC.1 FTP_TRP.1
FDP_RIP.1	
FDP_ROL.1	FDP_ACC.1
FDP_SDI.2	
FDP_UIT.1/Backup-archive	FDP_ACC.1 FTP_ITC.1
FDP_UIT.1/Audit-archive	FDP_ACC.1 FTP_ITC.1
FIA_AFL.1	FIA_UAU.1
FIA_ATD.1	
FIA_UAU.1	FIA_UID.1
FIA_UAU.5	
FIA_UAU.6	
FIA_UID.1	
FIA_USB.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1
FMT_MSA.1/Key-Regen	FDP_ACC.1 FMT_SMR.2 (Hierarchical to FMT_SMR.1) FMT_SMF.1
FMT_MSA.1/Signatory	FDP_ACC.1 FMT_SMR.2 (Hierarchical to FMT_SMR.1) FMT_SMF.1
FMT_MSA.3	FMT_MSA.1/Key-Regen FMT_MSA.1/Signatory

Requirement	Dependences
	FMT_SMR.1
FMT_SMF.1	
FMT_SMR.2	FIA_UID.1
FPT_TDC.1	
FPT_TST.1	
FTA_SSL.3	
FTA_SSL.4	
FTA_TSE.1	
FTP_ITC.1	
FTP_TRP.1	

Table 16: SFR dependency satisfaction mapping

5.3. Security Requirements Rationale

5.3.1. Security Requirements Coverage

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

SFR/Security Objectives	OT.Startup&Shutdown_Security	OT.SCD_Secure_Lifecycle	OT.Key_Secure_Management	OT.SigFunction_Usage	OT.Signatory_Auth	OT.Privileged_Auth	OT.Secure_Delegation	OT.Account_Separation	OT.Audit_Prot	OT.Backup_Prot	OT.Trusted_Comm
FAU_ARP.1	X			X	X	X	X				
FAU_GEN.1	X	X	X	X			X		X		
FAU_GEN.2	X	X	X	X			X		X		
FAU_SAA.1	X			X							
FAU_SAR.1									X		
FAU_SAR.2									X		
FAU_SAR.3									X		
FAU_STG.2									X		
FCS_CKM.4		X		X							
FCS_COP.1		X		X							
FDP_ACC.1/Management	X		X			X		X	X	X	
FDP_ACC.1/Signer		X		X	X		X	X			
FDP_ACF.1/Management	X		X			X		X	X	X	
FDP_ACF.1/Signer		X		X	X		X	X			
FDP_ETC.1	X	X	X	X	X	X	X			X	
FDP_ETC.2			X	X			X		X	X	
FDP_ITC.1		X	X	X	X	X				X	
FDP_ITC.2		X	X	X			X		X	X	
FDP_RIP.1		X	X	X	X	X	X				
FDP_ROL.1										X	
FDP_SDI.2		X		X			X				
FDP_UIT.1/Backup-archive										X	
FDP_UIT.1/Audit-archive									X		
FIA_AFL.1	X	X		X	X	X					
FIA_ATD.1					X	X					
FIA_UAU.1	X			X	X	X	X	X	X	X	
FIA_UAU.5				X	X						
FIA_UAU.6					X	X					
FIA_UID.1		X	X		X	X					
FIA_USB.1				X	X	X	X				
FMT_MOF.1	X		X					X	X	X	
FMT_MSA.1/Key-Regen			X								
FMT_MSA.1/Signatory		X		X			X				
FMT_MSA.3		X	X	X	X	X	X			X	
FMT_SMF.1	X		X					X	X	X	
FMT_SMR.2				X		X		X	X	X	
FPT_TDC.1		X	X	X			X		X	X	
FPT_TST.1	X										
FTA_SSL.3					X	X					

SFR/Security Objectives	OT.Startup&Shutdown_Security	OT.SCD_Secure_Lifecycle	OT.Key_Secure_Management	OT.SigFunction_Usage	OT.Signatory_Auth	OT.Privileged_Auth	OT.Secure_Delegation	OT.Account_Separation	OT.Audit_Prot	OT.Backup_Prot	OT.Trusted_Comm
FTA_SSL.4					X	X					
FTA_TSE.1		X	X	X	X	X	X		X	X	X
FTP_ITC.1		X	X	X	X	X	X		X	X	X
FTP_TRP.1			X		X	X					X

Table 17: Security Requirements Coverage

5.3.2. Security Requirements tracing justification

The following section provides justification for the above mapping.

OT.Startup&Shutdown_Security TOE secure start-up and shutdown

The test functions **FPT_TST.1** provide failure detection throughout the initial start-up.
FIA_UAU.1 ensures the user is authenticated before he can invoke the system start-up and initialization mode selection.

FDP_ACC.1/Management, FDP_ACF.1/Management, FMT_SMF.1 and **FMT_MOF.1** provide access to *Start-up* and *Shut-down* operations with restriction to *R.Administrator* and *R.Operator* roles.

FAU_GEN.1 and **FAU_GEN.2** provide assurance for audit data generation functionality on start-up and shutdown, and audit data reporting ensuring no data is lost on these processes. **FAU_SAA.1** analyzes this data and looks for any security related issue that may happen. If any issue is detected, **FAU_ARP.1** generates a security alarm and **FDP_ETC.1** send a warning notification to the receiver list configured on the system and user who generated the alert. If initial user authentication retries limit is reached **FIA_AFL.1** shuts down console interaction with the user.

OT.SCD_Secure_Lifecycle Security on SCD creation and destruction

FAU_GEN.1 and **FAU_GEN.2** provides audit data generation on creation and destruction of SCDs. **FCS_COP.1** defines the operation used on SAD generation.

FIA_UID.1 ensures that only authenticated users can access the related functionalities and **FIA_AFL.1** protects the access.

FDP_ACC.1/Signer, FDP_ACF.1/Signer, FDP_ETC.1, FMT_MSA.1/Signatory, FDP_ITC.1, FTA_TSE.1 and **FTP_ITC.1** ensure that *Certificate Request, Certificate Enroll, Certificate delete, Renovate qualified certificate, Policy edition, Certificate change pin* and *Delegate qualified signature* operations are performed in a secure way such that provides secure for creation, activation, deletion, renovation, modification and delegation *Qualified Certificate* along with its SCD.

FDP_ACC.1/Signer, FDP_ACF.1/Signer, FMT_MSA.1/Signatory, FDP_ITC.2, FPT_TDC.1, FTA_TSE.1, FTP_ITC.1 and **FDP_SDI.2** ensure that *Signature creation* operation are performed in a secure way such that provides secure *Signature* with *Advanced* or *Qualified Certificate* along with its SCD.

FCS_CKM.4 and **FDP_RIP.1** assures that a secure destruction of the sensible generated data (SAD and Static VAD) is performed correctly. **FMT_MSA.3** ensures default values of security attributes are *restrictive.*

OT.Key_Secure_Management Security on infrastructure and controls KEY management

FAU_GEN.1 and **FAU_GEN.2** provides audit data generation on regeneration of KEYs.

FMT_SMF.1 assures that Internal Key Regeneration functions are provided.

FIA_UID.1 and **FMT_MOF.1** ensures that only authenticated users with role R.Administrator can access the Internal Key Regeneration functions.

FDP_ACC.1/Management, FDP_ACF.1/Management, FDP_RIP.1, FMT_MSA.1/Key-Regen and **FDP_ITC.1** provides overall protection for the Internal Key Regeneration and protects the *KEYid/KEY pass* pair when it's passed between the R.Administrator and the TOE.

FDP_ACC.1/Management, FDP_ACF.1/Management, FDP_ETC.1, FDP_ETC.2, FDP_ITC.2, FMT_MSA.1/Key-Regen and **FPT_TDC.1** protects the concrete *Regenerate internal key* operatives in the paths of sensible security data between the TOE and the Database and between the TOE and the HSM.

FTA_TSE.1, FTP_ITC.1 and **FTP_TRP.1** assures that all subjects related to the Internal Key Regeneration operations performs their communications in a secure way (with confidentiality and integrity). **FMT_MSA.3** ensures default values of security attributes are *restrictive*.

OT.SigFunction_Usage	Signature creation function for the legitimate signatory

FIA_UAU.1 ensures no signature generation function can be invoked before a user is identified and authenticated. A double factor authentication is required for signature operation function, provided by **FIA_UAU.5**.

FDP_ACC.1/Signer, FDP_ACF.1/Signer and **FMT_MSA.1/Signatory** provide access to signature creation operation with restriction to roles *R.CertOwner* and *R.Signer* addressed by **FMT_SMR.2**. Additionally **FDP_ITC.2, FPT_TDC.1, FTA_TSE.1, FTP_ITC.1** and **FDP_SDI.2** ensure the signatory has access only to the SCD he's authorized to. **FIA_USB.1** guarantees that the authenticated user is the same that the user who realizes the signature operation.

Signature creation operation is initiated by *vinCERTagent* by means of a secure channel session establishment provided by **FTA_TSE.1**. On signature creation operation, **FMT_MSA.3** ensures default values of security attributes are *restrictive*, **FDP_ITC.1** provides protection for *data to be signed* and *Static VAD*'s integrity and confidentiality on its import from *vinCERTagent*, and **FCS_COP.1** provides security for the *PIN (Static VAD) derivation* cryptographic operation for *SAD* creation. The *SAD* (for *SCD* activation) and the *data to be signed* (*DTBS/R*) is sent to the HSM through a secure communication channel provided by **FDP_ETC.2** and **FTP_ITC.1**. Once the data is signed, **FDP_ITC.2**, **FPT_TDC.1** and **FTP_ITC.1** provide security for its import from HSM. Additionally, **FAU_GEN.1** and **FAU_GEN.2** provide assurance for every signature operation's audit data generation. For this data, **FAU_SAA.1** provides monitoring and may trigger a *warning notification* during *signature creation* operation (if any error is detected from it) provided by **FDP_ETC.1**, and perform a countermeasure provided by **FAU_ARP.1** in case the error is the SCD activation retries limit reaching.

As a prerequisite for a user to be able to use an *SCD* for signature, he/she must provide a PIN (*Static VAD*) for *SCD Activation*, **FIA_AFL.1** provides control over this process, and performs a countermeasure (disable the SCD) if the retries limit for this PIN verification is met.

FCS_CKM.4 provides a secure method for *SAD* deletion after its usage. Along with **FDP_RIP.1**, which provides security for ensuring no residual information content of any resource on *signature creation* is available after its use, both provide security for *signature creation* related data's confidentiality protection.

OT.Signatory_Auth	Signatory authentication based on multifactor authentication

OT.Signatory_Auth is provided by **FIA_UAU.1, FIA_UAU.5**, **FIA_UID.1, FIA_ATD.1** and **FIA_USB.1**. It is mandatory to present the both password and OTP before any digital signature operation. **FIA_UAU.6** ensures that after a log out, the TSF shall re-authenticate the user. **FTP_TRP.1** provides the trusted path.

FAU_ARP.1 generates a security alarm when a potential security violation is detected, **FIA_AFL.1** guarantees user's account locking after a several unsuccessful authentication attempts and **FDP_ETC.1** send a warning notification to inform the involved user, if exist, and configured list of warning event receivers.

FDP_ACC.1/Signer, FDP_ACF.1/Signer, FDP_ETC.1, FTA_TSE.1, FDP_ITC.1 and **FTP_ITC.1** assure secure export, import and data protection during credential validation (note that the secured RADIUS server communication isn't covered by **FTP_ITC.1** but by *OE.Secured_RADIUS*). Firstly the user credential validation is done against *Active Directory* and then the following OTP validations are done against a *RADIUS server*, only after the success of all validations the digital signature operation can be performed. The imported user-role relation data is protected by trusted channel communication. **FMT_MSA.3** ensures default values of security attributes are *restrictive*.

FDP_RIP.1 make the AD password and any other related information unavailable upon the deallocation of the information.

FTA_SSL.3 finishes a user's session after a time of inactivity and **FTA_SSL.4** allows the user to finish the user's own session.

OT.Privileged_Auth Privileged authentication prior to administrative operations

Only after a proper authentication by a trusted path, each user with privileged role defined in **FMT_SMR.2** can continue and perform administrative operations. A trusted path is provided by **FIA_UID.1** and **FTP_TRP.1**, while privileged authentication by **FIA_UAU.1, FIA_ATD.1** and **FIA_USB.1**.

FIA_UAU.6 assure that each user with privileged role shall be re-authenticate after log out.

FDP_ACC.1/Management, FDP_ACF.1/Management, **FDP_ITC.1, FTA_TSE.1** and **FTP_ITC.1** ensure *User Account* data is protected when it is validated against the *Active Directory*. Also, ensure that user credentials data and their account data imported from *Active Directory* are unambiguously associated. Altogether provide privileged authentication security for the *User Account*. **FMT_MSA.3** ensures default values of security attributes are *restrictive*.

If it's detected consecutive failed authentication attempts, **FIA_AFL.1** ensures locking the *User Account* in *Active Directory*. **FAU_ARP.1** generates a security alarm and **FDP_ETC.1** send a warning notification to inform the involved user, if exist, and configured list of warning event receivers.

FDP_RIP.1 make the AD password and any other related information unavailable upon the deallocation of the information.

FTA_SSL.3 finishes a user's session after a time of inactivity and **FTA_SSL.4** allows the user to finish the user's own session.

OT.Secure_Delegation Security on certificate delegation mechanisms

FIA_UAU.1 ensures the user is authenticated before he can perform or accept any SCD delegation or SCD delegation revocation. After the user is authenticated, *SCD delegation* is invoked from *vinCERTweb*, therefore, **FTA_TSE.1** provides a secure channel session establishment between this environment's element and the TOE. **FIA_USB.1** guarantees that the authenticated user is the same that the user who realizes the secure delegation operation.

FDP_ACC.1/Signer and **FDP_ACF.1/Signer** provide access control for the three TOE operatives related to SCD delegation: *Advanced Delegation*, *Qualified Delegation*, and *Accept Delegation*. For Advanced Delegation and Qualified delegation, **FMT_MSA.1/Signatory** restricts the user control over their security attributes management, and **FMT_MSA.3** provides restrictive default values for these attributes.

For the delegation operative itself, whether it's *Advanced Delegation* or *Qualified Delegation*, **FDP_ITC.2** and **FPT_TDC.1** provide integrity assurance for delegation policy data retrieval from database along with **FTP_ITC.1** which ensures a secure communication channel is stablished between the TOE and the environment's database. **FDP_ETC.2** provides assurance for policy data integrity on its exportation from the TOE to the environment's database for *Delegation Advanced* and *Delegation Qualified*.

On the delegation process, **FDP_SDI.2** provides monitoring and control for possible integrity errors on *user data* and *SCD* association. If an integrity error is detected or in case of error in the SCD activation retries limit reaching during the delegation procedure, **FAU_ARP.1** generates a security alarm and **FDP_ETC.1** send a warning notification to inform the involved user, if exist, and configured list of warning event receivers.

FDP_ACC.1/Signer and **FDP_ACF.1/Signer** provide access control assurance for *Revoke qualified delegation* operation of *qualified* signature delegation.

FAU_GEN.1 and **FAU_GEN.2** provide assurance for every delegation operation's audit data generation.

FDP_RIP.1 provides security for ensuring no residual information content of any resource on *SCD delegation* is available after its use.

OT.Account_Separation	Separation between different user accounts

FIA_UAU.1 ensures the user is authenticated before he can have access or invoke any of TOE's operatives.

FMT_SMR.2 restricts the separation between each role, along with **FMT_MOF.1**, which define every operation available for each one of the privileged roles (*R.Operator*, *R.Administrator*, *R.SecurityOfficer* and *R.Auditor*) from the complete operative's list defined by **FMT_SMF.1**, ensure that based on his/her role every TOE's authenticated user can only perform the operations he's allowed to.

FDP_ACC.1/Management and **FDP_ACF.1/Management** provide access control for *Generate backup, Restore system, Configure environment, Regenerate internal keys, Audit purge, Configure security, Audit review, Audit verify, Generate audit archive, Certificate delete, Policy edition* operations and also for the operations defined in **FMT_SMF.1** for users with roles *R.Administrator, R.Operator, R.SecurityOfficer* and *R.Auditor.*

FDP_ACC.1/Signer and **FDP_ACF.1/Signer** provide access control for *Certificate import, Certificate request, Certificate enroll, Certificate delete, Renovate advanced certificate, Renovate qualified certificate, Policy edition, Light policy delete, Certificate change pin, Delegate advanced signature, Delegate qualified signature, Revoke qualified delegation, Accept delegation* and *Signature creation* operations for users with roles *R.CertOwner* and *R.Signer.*

OT.Audit_Prot	Protection of the audit data

FAU_GEN.1 and **FAU_GEN.2** ensure adequate generation of audit records for a list of auditable events.

FAU_STG.2 provides ways to prevent unauthorized modifications to the stored audit records in the audit trail and avoid audit storage fail. **FDP_ETC.2** and **FTP_ITC.1** provides mechanisms to assure the integrity and safe storing of audit trail to be exported from TOE to database.

FIA_UAU.1 requires user authentication before allowing the audit functions access and **FMT_MOF.1**, **FMT_SMR.2** and **FMT_SMF.1** assures that only users with *R.Auditor* can perform the audit functions.

FAU_SAR.1, FAU_SAR.2, FAU_SAR.3 set policy control over which users can read the audit records. **FDP_ITC.2, FDP_ETC.2** and **FPT_TDC.1** ensures that the integrity of the *Audit trail* is correct when they are imported from database to TOE and when they are exported outside TOE, both for be reviewed by an *R.Auditor.*

The access to review and verify the *Audit records, and Audit archive* generation are controlled by **FDP_ACC.1/Management** and **FDP_ACF.1/Management**. Ensuring that the *Audit archive* integrity is correct when it's exported outside the TOE is provided by **FDP_ETC.2** and **FDP_UIT.1/Audit-archive**.

Secure channel session establishment between the TOE and the *SSH Client* is provided by **FTA_TSE.1. FTP_ITC.1** provides trusted channel to export audit archive.

OT.Backup_Prot	Backup data protection

FIA_UAU.1 requires user authentication before allowing the backup functions access. **FMT_MOF.1** defines every operation available for each role from the complete operative's list defined by **FMT_SMF.1** that ensures that every TOE's authenticated user can only perform the operations he's allowed based on his/her role. **FMT_SMR.2** ensure maintain the roles and a list of conditions in management roles.

The access to *Generate backup* and *Restore system* operatives to create and restore backups is provided by **FDP_ACC.1/Management** and **FDP_ACF.1/Management.**

FDP_ETC.2 guarantee integrity and confidentiality when exporting user's data with the user data's associated security attributes.

FDP_ITC.2 and **FPT_TDC.1** provides integrity and confidentiality when importing backup data from outside the TOE. Secure channel session establishment between the TOE and the *SSH Client* is provided by **FTA_TSE.1.**

FDP_ROL.1 enforce the restore system and the import backup to permit the rollback.

The ability to determine the modifications in the user data and protect it from modification errors is provided by **FDP_UIT.1/Backup-archive**.

When the TOE loads and saves the configuration, **FDP_ITC.1, FDP_ITC.2**, **FDP_ETC.1**, **FDP_ETC.2, FTP_ITC.1** and **FPT_TDC.1** provide the security in the communication between the TOE and the HSM. **FMT_MSA.3** ensures default values of security attributes are *restrictive*.

OT.Trusted_Comm	Trusted communication with external IT products

FTA_TSE.1 provides and enforces secure channel session establishment between the TOE and the external It products: vinCERTweb and SSH client.

FTP_ITC.1 and **FTP_TRP.1** provides and enforces the trusted communication channel between the TOE and the external trusted IT products: AD server, vinCERTcamgr, Mail server, HSM and Database.

5.3.3. Rationale for EAL4 augmented

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

ALC_FLR.2 Flaw reporting procedures

This dependence exceeds in the EAL4 assurance package.

6. TOE summary specification

6.1.Identification and authentication (TSF.IA)

The TOE uses Active Directory to identify and authorize TOE users. All operations that govern the TOE shall be authenticated, except the initial trusted path establishment against the TOE for TOE users. The TOE only sends user password to a valid, and well configured Active Directory.

For non-privileged users, the TOE requires an additional authentication step provided by an external authentication product. Non-privileged users must present an OTP in addition to its password to access to TOE. For privileged users, second authentication step is not mandatory. The validation of user's OTP is managed via Radius protocol against external authentication service. The TOE only sends user OTP to a valid, and well configured Radius Server.

SFRs related to Identification and authentication	
FIA_UID.1 Timing of identification	The user must establish a secure channel before starting the login. Then the user must be identified to start the login operation.
FIA_UAU.1 Timing of authentication	The user must establish a secure channel before starting the login. Then the user must present his credential in login operation.
FIA_ATD.1 User attribute definition FIA_USB.1 User-subject binding	User's security attributes retrieved from active directory are associated to the TOE user's identity and authentication credentials, allowing a unique matching.
FIA_UAU.5 Multiple authentication mechanisms	Users of the TOE (users with Signer and CertOwner roles) require 2-step authentication mechanism based on user name and password for the first step and OTP for the second. First step is verified with Active Directory while that the OTP is verified with an external authentication server that must be provided by Radius protocol. Privileged users' authentication (users with Auditor, Administrator, Operator and Security Officer roles) don't require multiple authentication, only a unique user name and password to authenticate to the system.
FIA_UAU.6 Re-authenticating	The TOE permits logout function and after that, the user must re-authenticate to perform any operation.
FIA_AFL.1 Authentication failure handling	The TOE manages failed authentication attempts by blocking the user account in Active Directory and by disconnecting console. The environment must manage the unlock operations (only by authorized roles).

SFRs related to Identification and authentication	
FDP_ACC.1/Management and FDP_ACC.1/Signer Subset access control for *First factor authentication* operation FDP_ACF.1/Management and FDP_ACF.1/Signer Security attribute based access control for *First factor authentication* operation FDP_ETC.1 Export of user data without security attributes FDP_ITC.1 Import of user data without security attributes	The TOE restricts the access to a valid, and well configured Active directory, and verifies it before sending the user credential to be validated. In login operation, the TOE exports the user and his credential to Active Directory to validate the user. The TOE retrieves the status and role of authenticated user from Active directory before any action. The TOE validates the user account through a protocol that handles the connection integrity.
FDP_ACC.1/Signer Subset access control for *Second factor authentication* operation FDP_ACF.1/Signer Security attribute based access control for *Second factor authentication* operation FDP_ETC.1 Export of user data without security attributes FDP_ITC.1 Import of user data without security attributes	The TOE restricts the access to a valid, well configured Radius server, and verifies it before sending the user OTP to be validated. The TOE exports the user id and his OTP to the Radius Server to validate the user with his Second authentication factor. The TOE retrieves the validation of the user OTP in 2-factor authentication. The TOE uses to validate the OTP through a protocol that handles the connection integrity.
FDP_RIP.1 Subset residual information protection	The TOE guarantees the deletion of the credentials used during all steps of authentication procedure.
FMT_MSA.3 Static attribute initialisation	The default values of security attributes are restrictive.

Table 18: SFRs related to Identification and authentication

6.2.Roles (TSF.Role)

Access control to the TOE is based on the concept of TOE users associated to roles. Each of every defined roles are configured with a set of permissions and/or restrictions about the operations and objects that it can (or cannot) access.

The TOE supports the following roles:

- Certificate Owner (R.CertOwner): user with the ability to manage the lifecycle of its certificates
- Signer (R.Signer): user with the ability to sign with its assigned certificates.

And the following privileged roles:

- Security Officer (R.SecurityOfficer): user with the overall responsibility for administering the implementation of the security policies and practices.
- System Administrator (R.Administrator): user with the ability to install, configure and maintain the TOE but by means of a controlled access to security-related information.
- System Operator (R.Operator): users responsible for operating the TOE on a day-to-day basis and are authorized to perform the system backup and recovery.
- System Auditor (R.Auditor): users authorized to view archives and audit logs of the TOE for purposes of auditing the operations of the system according to security policy.

System operators and system auditors have privileged roles but are not able to administer or configure the TOE.

SFRs related to Roles	
FMT_SMR.2 Restrictions on security roles	The TOE enforces the following user roles: - Certificate Owner - Signer And the following privileged roles: - Security Officers - System Administrators - System Operators - System Auditors Security officers and system administrators are privileged system users.
FMT_MOF.1 Management of security functions behaviour	The TOE manages the access control of the functions for privileged roles based on the Table 14: Function/Role mapping.

Table 19: SFRs related to Roles

6.3. Certificate and key-pair lifecycle (TSF.CertSign)

The vinCERTcore manages the following operations around Certificate and in case of be protected by key, its associated key-pair:

- *Certificate lifecycle:* The TOE allows the following operations:
  - *Certificate import*
  - *Certificate request*
  - *Certificate enroll*
  - *Certificate delete*
  - *Renovate advanced certificate*
  - *Renovate qualified certificate*
  - *Policy edition*
  - *Light policy delete*
  - *Certificate change pin*

- *Signature Delegation*: The TOE permits to delegate the ability to sign with one certificate to other users with the previous Certificate Owner acceptance. Operations related to the delegation are:
  - *Delegate advanced signature*
  - *Delegate qualified signature*
  - *Revoke qualified delegation*

- *Secure Signature*: The TOE permits to the authorized users perform cryptographic operations.

6.3.1. Key protection

Certificates generated with the TOE are protected with one key generated from static data retrieved from user (static VAD):

SFRs related to Key protection	
FCS_COP.1 Cryptographic operation	User keys generated in the external HSM for the TOE's Certificate Request are protected with a key (Signature activation data). This key is derived from user's static VAD provided by the user in the signature process. The derivation function is based on algorithm PBKDF2 described in [9].
FCS_CKM.4 Cryptographic key destruction	The derivate key that protects the user key-pair is deleted from memory once it is activated with mechanism described in [8].
FMT_MSA.3 Static attribute initialisation	The TOE restricts the default values of imported data related to certificate operations: - Certificate-Request - Certificate-Enroll - Renovate advanced certificate - Renovate qualified certificate - Delegation-Advanced - Delegation-Qualified - Signature-creation

Table 20: SFRs related to Key protection

6.3.2. Certificate lifecycle

In this section are described the following operations:

- *Certificate import*: This operation allows import an existing software certificate from outside of the TOE. One user with Certificate Owner role can import software Certificates to vinCERTcore.

- *Certificate request*: This operation allows generate qualified certificate. One user with Certificate Owner role can request one certificate. In this operation, the TOE requests to the HSM a generation of a key-pair. The key-pair is protected with derivate of static data provided by user at start of the operation. Then the TOE generates a Certificate Request based on the configured certificate profile selected by user and sends the request to external CA.

- *Certificate enroll*: Once the CA finishes to issue the certificate, the user proceeds to enroll retrieved certificate to its key-pair.

- *Certificate delete*: One user with Certificate Owner role can delete his certificates and the associated key-pair. Administrator role user can delete any existing certificate and the associated key-pair, without pin provided. When a certificate is deleted, all policies associated are deleted too.

- *Renovate advanced certificate:* One user with Certificate Owner role can renovate its imported certificate. User must be owner of the certificate. For that, it consults its import ownership policy associated. User imports an existing software certificate from outside of the TOE. Policies from original certificate are associated to new certificate.

- *Renovate qualified certificate:* One user with Certificate Owner role can renovate its generated certificate. User must be owner of the certificate. For that, it consults its import ownership policy associated. It's performing certificate request operation with the same values of original certificate. It generated a new qualified certificate.

- *Policy edition:* One user with Certificate Owner role can modify policies related with its own certificates. If the certificate is advanced but is protected by key or is qualified, user must provide a static VAD which protects the key-pair. In addition, policy status of qualified certificates must be none or delegated. Administrator role or Operator role user can only modify the idAcl field in 'modify policies' operation.

- *Light policy delete:* One user with Certificate Owner role can delete policies related with its own imported certificates.

- *Certificate change pin:* One user with Certificate Owner or Signer role can change pin of its policy associated. If the certificate is advanced but is protected by key or is qualified, user must provide old static VAD which protects the key-pair. Once key-pair is validated, the TOE requests to the HSM a generation of a key-pair. The key-pair is protected with derivate of new static VAD. In case that advanced certificate is not protected by key, it is not necessary key-pair validation with old static VAD.

SFRs related to Certificate lifecycle	
FDP_ACC.1/Signer Subset access control for *Certificate import* operation FDP_ACF.1/Signer Security attribute based access control for *Certificate import* operation	Access control to Certificate Import operation is restricted to users with CertOwner role. Users with CertOwner role must be correctly authenticated with 2-factor authentication. TOE supports imported certificates encapsulated in a PKCS#12 file format as is described in [10]

SFRs related to Certificate lifecycle	
FDP_ITC.1 Import of user data without security attributes for *Certificate import* operation	User imports the certificate and its key-pair from outside of the TOE specifying PKCS#12 file and it's secret.
FDP_ETC.1 Export of user data without security attributes for *Certificate import* operation	The TOE loads the certificate and its key-pair into HSM providing the secret to open PKCS#12 file.
FDP_ACC.1/Signer Subset access control for *Certificate request* operation FDP_ACF.1/Signer Security attribute based access control for *Certificate request* operation	Access control to Certificate Request operation is restricted to users with CertOwner role. Users with CertOwner role must be correctly authenticated with 2-factor authentication. When the TOE processes Certificate Request operation, user must enter the static VAD and select one of the available certificate profiles configured in the TOE. Then the TOE requests to HSM the generation of a key-pair protected with key derivate [9] from static VAD. Additionally, the TOE generates a PKCS#10 based on [11] to send to CA infrastructure requesting the certificate.
FDP_ETC.1 Export of user data without security attributes for *Certificate request* operation	The TOE sends a request to CA, through vinCERTcamgr, with PKCS#10 [11] file.
FMT_MSA.1/Signatory Management of security attributes for *create* ability	The TOE restricts the ability to *create* the security attributes of Certificate Request to the user with CertOwner role.
FDP_ACC.1/Signer Subset access control for *Certificate enroll* operation FDP_ACF.1/Signer Security attribute based access control for *Certificate enroll* operation	Access control to Certificate Enroll operation is restricted to users with CertOwner role that have initiated Certificate Request operation. Users with CertOwner role must be correctly authenticated with 2-factor authentication. When the TOE processes certificate Enroll operation, user must enter the static VAD used in Certificate Request operation to activate the key-pair as proof that the key is associated to the user.
FDP_ITC.1 Import of user data without security attributes for *Certificate enroll* operation	In Certificate Enroll operation, the TOE retrieves the certificate data from CA. The TOE verifies the correspondence between certificate and key-pair to process the operation.

SFRs related to Certificate lifecycle	
FMT_MSA.1/Signatory Management of security attributes for *modify* ability	The initialization data of certificate structure is restricted to CertOwner.
FDP_ACC.1/Management Subset access control for *Certificate delete* operation FDP_ACF.1/Management Security attribute based access control for *Certificate delete* operation FDP_ACC.1/Signer Subset access control for *Certificate delete* operation FDP_ACF.1/Signer Security attribute based access control for *Certificate delete* operation	Access control to Certificate Delete operation is restricted to users with CertOwner or Administrator role having valid certificate and its associated key-pair. Users with CertOwner or Administrator role must be correctly authenticated with 2-factor authentication. For CertOwner role users, in case of certificates generated with the TOE, user must provide the static VAD to enable the key. In case of imported certificates, this step is not required. For Administrator role users, static VAD is not required in no case.
FDP_ITC.2 Import of user data with security attributes FPT_TDC.1 Inter-TSF basic TSF data consistency	User only can renovate own certificates. The TOE retrieves light policies from external database to check ownership policy associated. The TOE verifies the *policy integrity* for each imported light policy by verifying the digital signature of each policy.
FDP_ACC.1/Signer Subset access control for *Renovate advanced certificate* operation FDP_ACF.1/Signer Security attribute based access control for *Renovate advanced certificate* operation	Access control to Renovate advanced certificate operation is restricted to users with CertOwner role. Users with CertOwner role must be correctly authenticated with 2-factor authentication.
FDP_ITC.2 Import of user data with security attributes FPT_TDC.1 Inter-TSF basic TSF data consistency	User only can renovate own certificates. The TOE retrieves light policies from external database to check ownership policy associated. The TOE verifies the *policy integrity* for each imported policy by verifying the digital signature of each policy.
FDP_ITC.1 Import of user data without security attributes for *Renovate advanced certificate* operation	TOE supports imported certificates encapsulated in a PKCS#12 file format as is described in [10] User imports the certificate and its key-pair from outside of the TOE specifying PKCS#12 file and it's secret.

SFRs related to Certificate lifecycle	
FDP_ETC.1 Export of user data without security attributes for *Renovate advanced certificate* operation	The TOE loads the certificate and its key-pair into HSM providing the secret to open PKCS#12 file.
FDP_ACC.1/Signer Subset access control for *Renovate qualified certificate* operation FDP_ACF.1/Signer Security attribute based access control for *Renovate qualified certificate* operation	Access control to Renovate qualified certificate operation is restricted to users with CertOwner role. Users with CertOwner role must be correctly authenticated with 2-factor authentication. When the TOE processes Renovate qualified certificate operation, user must enter the static VAD. Certificate profile is the same that original certificate. Then the TOE requests to HSM the generation of a key-pair protected with key derivate [9] from static VAD. Additionally, the TOE generates a PKCS#10 based on [11] to send to CA infrastructure requesting the certificate.
FDP_ITC.2 Import of user data with security attributes FPT_TDC.1 Inter-TSF basic TSF data consistency	User only can renovate own certificates. The TOE retrieves strong policies from external database to check ownership policy associated. The TOE verifies the *policy integrity* for each imported policy by verifying the digital signature of each policy.
FDP_ETC.1 Export of user data without security attributes for *Renovate qualified certificate* operation	The TOE sends a request to CA, through vinCERTcamgr, with PKCS#10 [11] file.
FMT_MSA.1/Signatory Management of security attributes for *create* ability	The TOE restricts the ability to *create* the security attributes of Renovate qualified certificate to the user with CertOwner role.
FDP_ACC.1/Management Subset access control for *Policy edition* operation FDP_ACF.1/Management Security attribute based access control for *Policy edition* operation FDP_ACC.1/Signer Subset access control for *Policy edition* operation FDP_ACF.1/Signer Security attribute based access control for *Policy edition* operation	Access control to Policy edition operation is restricted to users with CertOwner role, Administrator role and Operator role. Users with CertOwner role must have a valid certificate and its associated key-pair if necessary. Users with Administrator role and Operator role, can only modify the idAcl field. Users with CertOwner role, Administrator role and Operator role must be correctly authenticated with 2-factor authentication.

SFRs related to Certificate lifecycle	
	When the TOE processes Policy edition operation with CertOwner role, if the certificate is advanced but is protected by key or is qualified, user must enter the static VAD. Then the TOE requests to HSM the generation of a key-pair protected with key derivate [9] from static VAD. When the TOE processes Policy edition operation with Administrator or Operator role, idAcl update don't need static VAD parameter.
FDP_ITC.2 Import of user data with security attributes FPT_TDC.1 Inter-TSF basic TSF data consistency	CertOwner user only can modify policies related with its own certificates. The TOE retrieves light or strong policies from external database to check ownership policy associated. Administrator or Operator user can only modify the idAcl field in all policies. The TOE retrieves all policies from external database. The TOE verifies the *policy integrity* for each imported policy by verifying the digital signature of each policy.
FDP_ETC.2 Export of user data with security attributes	Once policy is modified, it is stored in database. Policies have an attribute to guarantee the policy integrity. The integrity attribute is generated by signing the policy data with database integrity asymmetric key.
FMT_MSA.1/Signatory Management of security attributes for *modify* ability	The TOE restricts the ability to *modify* the security attributes of Light and Strong policies to the user with CertOwner role.
FDP_ACC.1/Signer Subset access control for *Light policy delete* operation FDP_ACF.1/Signer Security attribute based access control for *Light policy delete* operation	Access control to Light policy delete operation is restricted to users with CertOwner role having valid certificate and its associated key-pair if necessary. Users with CertOwner role must be correctly authenticated with 2-factor authentication. When the TOE processes Light policy delete operation, if the certificate is advanced but is protected by key or is qualified, user must enter the static VAD. Then the TOE requests to HSM the generation of a key-pair protected with key derivate [9] from static VAD.

SFRs related to Certificate lifecycle	
FDP_ITC.2 Import of user data with security attributes FPT_TDC.1 Inter-TSF basic TSF data consistency	User only can *delete* policies related with its own certificates. The TOE retrieves light policy from external database to check ownership policy associated. The TOE verifies the *policy integrity* for each imported policy by verifying the digital signature of each policy.
FMT_MSA.1/Signatory Management of security attributes for *delete* ability	The TOE restricts the ability *delete* the security attributes of Light policies to the user with CertOwner role.
FDP_ACC.1/Signer Subset access control for *Certificate change pin* operation FDP_ACF.1/Signer Security attribute based access control for *Certificate change pin* operation	Access control to Certificate change pin operation is restricted to users with CertOwner or Signer role having valid certificate and its associated key-pair if necessary. Users with CertOwner role must be correctly authenticated with 2-factor authentication. When the TOE processes Certificate change pin operation, if the certificate is advanced but is protected by key or is qualified, user must enter old static VAD. Then the TOE validate to HSM the key-pair protected with key derivate [9] from old static VAD. For all cases, user must enter new static VAD. Then the TOE requests to HSM the generation of a key-pair protected with key derivate [9] from new static VAD.
FDP_ITC.2 Import of user data with security attributes FPT_TDC.1 Inter-TSF basic TSF data consistency	User only can *modify* own policies pin. The TOE retrieves light or strong policies from external database to check own policies. The TOE verifies the *policy integrity* for each imported policy by verifying the digital signature of each policy.
FMT_MSA.3 Static attribute initialisation	The TOE restricts the default values of imported data related to certificate operations: - Certificate-Request - Certificate-Enroll - Renovate advanced certificate - Renovate qualified certificate

Table 21: SFRs related to Certificate lifecycle

6.3.3. Signature delegation

The signature delegation operation refers to delegate the ability to sign with certificates managed by vinCERTcore. There are two mechanisms to delegate signature capability:

- *Delegate advanced signature*: To delegate signature for imported certificates.
  Imported recognized software certificates generates Advanced Signature. In the delegation process, owner of the certificate can generate light policies to delegate signature to users with Signer role. Multiple light policies can be generated in this kind of delegation.
  Additionally, light policies can be configured with PIN activation before signature creation operation.

- *Delegate qualified signature*: To delegate signature for generated certificates.
  Recognized certificates issued by the TOE generate Qualified Signature. In the delegation process, owner of the certificate can delegate signature to single user, that is, only a unique pair Qualified Signature/Signer can exists with Signer role. The delegation is managed with strong policies.

  Only one strong policy can be assigned to one certificate of this kind and needs to be approved by target signer to enable the policy. After the signer accept the usage of certificate, the signer can generate qualified signature in name of Certificate Owner.

  During the *Qualified signature delegation* operation, a backup of key-pair is generated to allow the *Revoke qualified delegation* operation.

  The strong policies always require a static VAD (known only by user) to activate signature creation operation.

- *Revoke qualified delegation*: Reclaims the control of signature creation by Certificate Owner. Certificates with a delegated strong policy can be recovered by order of Certificate Owner using the key backup generated in *qualified signature delegation* operation. To start the operation, the Certificate Owner must enter new static VAD to activate the key for signature operation.

SFRs related to signature delegation	
FDP_ACC.1/Signer Subset access control for *Delegate advanced signature* operation FDP_ACF.1/Signer Security attribute based access control for *Delegation advanced signature* operation	Access control to Delegate Advanced Signature operation is restricted to users with CertOwner role to users with CertOwner and Signer roles. Users with CertOwner role must be correctly authenticated with 2-factor authentication. When the TOE processes the delegate advanced operation, the TOE verifies user security attributes.
FMT_MSA.1/Signatory Management of security attributes for *modify* abilities	Modification of policies security attributes are restricted to user with CertOwner role.
FDP_ITC.2 Import of user data with security attributes with *Light policy* object FPT_TDC.1 Inter-TSF basic TSF data consistency	User only can delegate advanced signature for own imported certificates. The TOE retrieves light policies from external database to check ownership policy associated. The TOE verifies the *policy integrity* for each imported light policy by verifying the digital signature of each policy.

SFRs related to signature delegation	
FDP_ETC.2 Export of user data with security attributes with *Light policy* object	Light policies have an attribute to guarantee the policy integrity. The integrity attribute is generated by signing the policy data with database integrity asymmetric key.
FDP_ACC.1/Signer Subset access control for *Delegate qualified signature* operation FDP_ACF.1/Signer Security attribute based access control for *Delegate qualified signature* operation	Access control to Delegation Qualified Signature operation is restricted to users with CertOwner role to users with CertOwner and Signer roles. Users with CertOwner role must be correctly authenticated with 2-factor authentication. When the TOE processes the delegate qualified signature operation, the TOE verifies user security attributes. The user must present the static VAD that protects the key in HSM in order to modify the policy.
FMT_MSA.1/Signatory Management of security attributes for *modify* abilities	Modification of policies security attributes are restricted to user with CertOwner role.
FDP_ITC.2 Import of user data with security attributes with *Strong policy* object FPT_TDC.1 Inter-TSF basic TSF data consistency	User only can delegate qualified signature for own generated certificates. The TOE retrieves strong policies from external database to check ownership policy associated. The TOE verifies the *policy integrity* for each imported strong policy by verifying the digital signature of each policy.
FDP_ETC.2 Export of user data with security attributes with *Strong policy* object	Strong policies have an attribute to guarantee the policy integrity. The integrity attribute is generated by signing the policy data with database integrity asymmetric key. Additionally, strong policies have integrity related to SCDid and user associated.
FDP_ACC.1/Signer Subset access control for *Accept delegation* operation FDP_ACF.1/Signer Security attribute based access control for *Accept delegation* operation	Access control to Accept Delegation operation is restricted to users with CertOwner and Signer roles that have an associated Strong Policy. Users with CertOwner and Signer roles must be correctly authenticated with 2-factor authentication. When the TOE processes the accept delegation operation, the TOE verifies user security attributes. The user must present the static VAD that protects the key in HSM in order to activate the policy.

SFRs related to signature delegation	
FDP_ITC.2 Import of user data with security attributes with *Strong policy* object FPT_TDC.1 Inter-TSF basic TSF data consistency	The TOE retrieves strong policies associated with qualified delegation from external database. The TOE verifies the *policy integrity* for each imported light policy by verifying the digital signature of each policy.
FMT_MSA.1/Signatory Management of security attributes for *modify* ability	Modification of policies security attributes are restricted to user with CertOwner role.
FDP_ACC.1/Signer Subset access control for *Revoke qualified delegation* operation FDP_ACF.1/Signer Security attribute based access control for *Revoke qualified delegation* operation	Access control to Revoke Qualified Delegation operation is restricted to users with CertOwner role that have an delegate qualified signature. Users with CertOwner role must be correctly authenticated with 2-factor authentication. When the TOE processes the revoke qualified delegation operation, the TOE verifies user security attributes. The user must present the static VAD that protects the key in HSM in order to modify the policy.
FMT_MSA.1/Signatory Management of security attributes for *modify* abilities	Modification of policies security attributes are restricted to user with CertOwner role.
FDP_ITC.2 Import of user data with security attributes with *Strong policy* object FPT_TDC.1 Inter-TSF basic TSF data consistency	User only can revoke qualified delegation for own generated certificates that have an delegate qualified signature. The TOE retrieves strong policies from external database to check ownership policy associated. The TOE verifies the *policy integrity* for each imported strong policy by verifying the digital signature of each policy.
FDP_ETC.2 Export of user data with security attributes with *Strong policy* object	Strong policies have an attribute to guarantee the policy integrity. The integrity attribute is generated by signing the policy data with database integrity asymmetric key. Additionally, strong policies have integrity related to SCDid and user associated.
FMT_MSA.3 Static attribute initialisation	The TOE restricts the default values of imported data related to certificate operations: - Delegation-Advanced - Delegation-Qualified - Revoke-Qualified-Delegation

Table 22: SFRs related to signature delegation

6.3.4. Secure signature

The TOE sends data to be signed (DTBS/R) to configured HSM (secure SCD) in order to generate its digital signature. Depending on the origin of used certificate, the TOE can return to the user two types of digital signature:

- *Advanced digital signature*: Generated when the signature operation is managed with certificates and its associated key-pair are imported from outside of the TOE.
- *Qualified digital signature*: Generated when the signature operation is managed with certificates and its associated key pair are generated within the TOE.

SFRs related to signature creation	
FDP_ACC.1/Signer Subset access control for *Signature creation* operation FDP_ACF.1/Signer Security attribute based access control for *Signature creation* operation	The TOE guarantees that only users with Signer roles (in case of delegated signature) or CertOwner (in case of key proprietary) can generate signature with keys associated. The access control checks user information at repositories and verifies the policy integrity of each binding user/SCDid mapped in the signature policy.
FDP_ITC.2 Import of user data with security attributes FPT_TDC.1 Inter-TSF basic TSF data consistency	The TOE retrieves signature policies from external database. The TOE verifies the *policy integrity* for each imported policy by verifying the digital signature of each policy.
FDP_SDI.2 Stores data integrity monitoring and action with *Light policy* object	Light policies are associated to imported certificates. One certificate and its associated key-pair can manage a couple of light-policies, each one associated to one user or group. During the life of the policy inside of the system, the TOE monitories the policy integrity to detect illegal modifications in the policy. In case to detect security violations related to policy integrity, the TOE blocks the user key, the system discards current operation and the TOE sends a notification to user and authorized security staff.

SFRs related to signature creation	
FDP_SDI.2 Stores data integrity monitoring and action with *Strong policy* object	Strong policies are associated to generated certificates. One certificate of this kind and its associated key-pair can only handle one strong-policy at time. During the life of the policy inside of the system, the TOE monitories the policy integrity to detect illegal modifications in the policy. Additionally, strong policies have additional SCDid/user id integrity control. In case to detect security violations related to policy integrity, the system discards current operation, blocks the user key and send a notification to user and authorized security staff.
FDP_ITC.1 Import of user data without security attributes for *Signature creation* operation	The TOE imports the data to be signed from vinCERTagent. In order to activate strong policies, a user must enter the key activation secret. This secret is used to generate the key used to activate the key-pair in HSM.
FDP_ETC.1 Export of user data with security attributes for *Signature creation* operation FDP_ITC.2 Import of user data with security attributes for *Signature creation* operation	Data to be signed is sent to HSM in order to *retrieve signed data.*
FPT_TDC.1 Inter-TSF basic TSF data consistency	*Signed data* is verified with its public SVD (public key associated) in order to verify that the correct key has signed the data.
FMT_MSA.1/Signatory Management of security attributes for *use to sign* ability	Key-pair identifier (SCDid) only can be used by authorized users with the roles Signer or CertOwner and used for the operation of *signature* creation.
FMT_MSA.3 Static attribute initialisation	The TOE restricts the default values of imported data related to certificate operations: - Signature-creation

Table 23: SFRs related to signature creation

6.4. Audit (TSF.Audit)

A complete deployment of vinCERTcore generates the following log types:

- *Application logs*, produced by the TOE for tracking problems or maintenance purposes. Since these logs are solely for monitoring and maintenance purposes, they are not cryptographically protected;
- *Audit logs*, produced by the TOE for security relevant events. Each log entry contains audit relevant data and is cryptographically protected by the TOE;
- *System logs*, produced by the IT environment supporting the TOE (e.g., Operating System, Database, HSM).

6.4.1. Audit generation and storage

Audit logs are of particular importance for security audits as reliable supporting evidence of operations. Log entries are produced whenever security relevant events (described in section 6.1.1) occur during execution of operations in the TOE and contain the following information:

- TOE User: Identification of the TOE user that originated the event;
- Date/time;
- Event Type: Description of the event (e.g. certificate issuance, key generation, etc.);
- Result: Description of the result type (OK or error);
- Module;
- Other relevant details.

Initially, the audit logs are stored within the TOE. With a periodic process, the TOE audit records transferred to external database secured properly by the environment.

This measure is taken to avoid any loss of audit data during execution of the TOE because of connectivity possible failures to the database.

After successful audit data is moved to database, the TOE removes internal audit data to prevent excess data in the file system.

The integrity of the audit logs stored in internal sore, in the database and on the export files is cryptographically protected, that not only ensure data authenticity, but also prevents undetected log entry deletion.

An error that prevents the persistence of audit logs cause that the TOE avoids execution of operations without properly recording related audit data.

Date and time accuracy of audit logs is guaranteed by requiring the IT environment to have system time synchronized with a reliable time source. The time source is considered reliable if is synchronized to within 1 second of Co-ordinated Universal Time (UTC).

The following table details the rationale applied to the usage of audit security requirements.

SFRs related to audit storage	
FAU_GEN.1 Audit data generation	Audit logs are generated along the occurrence of the events and immediately committed and stored inside the TOE. Later the audit registers are transmitted to database that is part of the IT environment.
FAU_GEN.2 User identity association	Audit logs include information about the TOE user identity.

SFRs related to audit storage	
FAU_STG.2 Guarantees of audit data availability	Audit logs are cryptographically protected against tampering and deletion. Additionally, all audit logs are maintained in case of connection failure with database.
FDP_ETC.2 Export of user data with security attributes	The TOE transmits audit data to external database in order to prevent system memory exhaustion. The audit data is transmitted to external database verifying the integrity of audit data and its digital signature.

Table 24: SFRs related to audit storage

6.4.2. Audit access control and review

VinCERTcore provides an interface to query, view and check the audit logs stored in the database. Additionally, vinCERTweb (another IT trusted product) can interact with the TOE to offer a web interface to query audit data.

During the audit review procedure, the TOE retrieves audit data from external database and verifies its integrity.

When the auditor prefers to use a web view, the TOE exports audit data to vinCERTweb to facilitate the audit review procedure.

SFRs related to audit review	
FAU_SAR.1 Audit review FAU_SAR.2 Restricted audit review FAU_SAR.3 Selectable audit review	The TOE provides a searching interface where audit logs can be queried by applying a configurable composition of criteria to users with Auditor role.
FDP_ACC.1/Management Subset access control for *Audit review* operation FDP_ACF.1/Management Security attribute based access control for *Audit review* operation	The TOE controls the access to the audit data to users with Auditor role.
FDP_ITC.2 Import of user data with security attributes	In order to show audit records, the TOE retrieves audit data from external database.

SFRs related to audit review	
FPT_TDC.1 Inter-TSF basic TSF data consistency	Audit records retrieved from database are verified before showing to the auditor in order to detect modifications or tampering in audit events.
FDP_ETC.2 Export of user data with security attributes	The auditor can inspect audit trail from TOE's Console or from vinCERTweb (an external trusted IT product). When the auditor uses vinCERTweb to search across the audit data, audit data is sent back to web.

Table 25: SFRs related to audit review

6.4.3. Audit archiving and verification

The vinCERTcore provides a Console operation to verify the integrity of audit trail stored in database. Also, user with Audit role can generate audit archive that could export outside TOE. Additionally, vinCERTweb (another IT trusted product of environment) can interact with the TOE to offer a web interface to query audit data.

When the auditor prefers to use a web view, the TOE exports audit data to vinCERTweb to facilitate the audit review procedure.

SFRs related to audit archiving and verification	
FDP_ACC.1/Management Subset access control for *Audit verify* operation FDP_ACF.1/Management Security attribute based access control for *Audit verify* operation	The TOE provides a Console operation to start the verification of the audit trail. The audit verify operation can be called by privileged users with role Auditor. The verification procedure checks each stored record verifying audit signature and integrity.
FDP_ACC.1/Management Subset access control for *Generate audit archive* operation FDP_ACF.1/Management Security attribute based access control for *Generate audit archive* operation	The TOE provides a Console operation to start the export of archive with a block of audit trail. The audit archive operation can be called by privileged users with role Auditor. The audit archive procedure retrieves audit blocks and prepares the audit archive file signed to prevent further modifications.
FDP_ETC.2 Export of user data with security attributes	The exported *audit archive* file contains all data related to audit registers to guarantee its integrity.
FDP_UIT.1/Audit-archive Data exchange integrity	The audit archive procedure generates one audit archive file *signed* to prevent further modifications in the file.

Table 26: SFRs related to audit archiving and verification

6.4.4. Audit analysis and warning notifications

The TOE continuously reviews the audit data searching possible security violations in the following scenarios:

- *Authentication failure events*
- *Private key activation failure events*

SFRs related to audit analysis and warnings	
FAU_SAA.1 Potential violation analysis	The TOE monitories two type of failed actions: - Login failures - SCD activation failures When an accumulation of these types of events occur, the TOE activates the procedures described in: - FAU_ARP.1
FAU_ARP.1 Security alarms	When the TOE detects a potential security violation in logon operation ((multiple login attempts in a short period, or multiple login attempts with invalid user ids) or SCD activation operation (multiple SCD activation attempts in a short period), TOE notifies via mail the potential security violation to involved user and system administrators. For SCD activation operation, also it deactivates the SDC policy to prevent further attacks. The CertOwner can reactivate the key from web interface.
FTP_ITC.1 Inter-TSF trusted channel FDP_ETC.1 Export of user data without security attributes	The TOE sends notifications to users using a secure SMTP server provided by the organization (IT environment).

Table 27: SFRs related to audit analysis and warnings

6.5.Admin functions (TSF.Admin)

The vinCERTcore provides the following administrative functions:

- *Start-up*: Once the service that manages the TOE is started, an administrator or operator must connect to console to start-up the TOE.
- *Shutdown*: The operator and administrator can stop the system.
- *Generate backup*: The operator and administrator can generate a backup of the TOE.
- *Restore system*: The operator and administrator can generate a backup of the TOE.
- *Configure environment parameters*: The administrator can configure the environment configuration related to:
    - Active Directory connection
    - Database connection
    - PKI connection *(vinCERTcamgr)*
    - Radius Server connection
    - SMTPS-Server connection
- *Configure security parameters*: The security officer can configure the security configuration related to:
    - Cryptographic algorithms and key supported key lengths
    - Certificate profiles
- *Regenerate keys*: The administrator can request the regeneration of infrastructure and control keys.
- *Audit purge*: The administrator can delete audit entries blocks from database once have been exported to external audit archive.
- *Generate audit archive*: The auditor can request the audit archive operation

SFRs related to admin functions	
FMT_SMF.1 Specification of Management Functions	The following operations are offered by the TOE using a SSH Console to privileged roles: - Generate backup - Restore system - Start-up the TOE - Shut-down the TOE - Configure environment - Regenerate Internal Keys - Audit purge - Configure security - Review audit records - Verify audit trail - Generate audit archive
FDP_ACC.1/Management Subset access control for *operations defined in FMT_SMF.1* FDP_ACF.1/Management Security attribute based access control for *operations defined in FMT_SMF.1*	The TOE controls the access to administrative functions based on role of logged privileged user following the Table 14: Function/Role mapping

Table 28: SFRs related to admin functions

6.5.1. Configure environment and security

Configure environment parameters: The administrator can configure the environment configuration related to:

- Active Directory connection
- Database connection
- PKI connection *(vinCERTcamgr)*
- Radius Server connection
- SMTPS-Server connection

Configure security parameters: The security officer can configure the security configuration related to:

- Cryptographic algorithms and key supported key lengths
- Certificate profiles

Modifications in TOE configuration are signed and encrypted with the key of configuration control.

SFRs related to configure environment and configure security	
FDP_ACC.1/Management Subset access control for *Configure environment* operation FDP_ACF.1/Management Security attribute based access control for *Configure environment* operation	The TOE controls and limits the access to Configure environment operation to Users with Administrator role. The TOE verifies the user account status and its role before processing the configure environment operation.
FDP_ACC.1/Management Subset access control for *Configure security* operation FDP_ACF.1/Management Security attribute based access control for *Configure security* operation	The TOE controls and limits the access to Configure security operation to Users with Security Officer role. The TOE verifies the user account status and its role before processing the configure environment operation.
FDP_ETC.2 Export of user data with security attributes for *Configure environment* and *Configure security* operations	During the save operation of the TOE's Configuration environment and Configure security, the system sends the configuration to the HSM for signing and encrypting with the key of configuration control.
FDP_ITC.1 Import of user data without security attributes for *Configure environment* and *Configure security* operations	The configuration of the TOE is retrieved, ciphered and signed, from the HSM. Then the configuration is saved in TOE's filesystem.

Table 29: SFRs related to configure environment and configure security

6.5.2. Audit purge

The administrator can delete audit entries blocks from database once have been exported to external audit archive.

SFRs related to audit purge	
FDP_ACC.1/Management Subset access control for *Audit purge* operation FDP_ACF.1/Management Security attribute based access control for *Audit purge* operation	The TOE controls and limits the access to Audit purge operation to Users with Administrator role. The TOE verifies the user account status and its role before processing the audit purge operation.
FDP_ITC.2 Import of user data with security attributes for *Audit purge* operation.	The audit end block number of the TOE is retrieved from external database.

Table 30: SFRs related to audit purge

6.5.3. Infrastructure and control keys management

The TOE uses the following infrastructure and control keys to guarantee the security and integrity of the data used by TOE:

- *Audit integrity key*: The audit key is an asymmetric key-pair and is used to sign and verify all audit actions during the lifecycle of the TOE.

- *Session management key*: The session management key is a symmetric key that secures the session tokens sent to TOE users.

- *Configuration key*: The Configuration key is an asymmetric key-pair and is used to sign, cipher, decipher and verify the configuration data and the backup operations.

- *Database integrity key*: The database integrity key is an asymmetric key-pair and is used to sign and verify all policies actions during the lifecycle of the TOE

SFRs related to key regeneration	
FDP_ACC.1/Management Subset access control for *Regenerate key* operation applied to *other infrastructure and control keys* FDP_ACF.1/Management Security attribute based access control for *Regenerate key* operation applied to *other infrastructure and control keys*	The TOE controls the access to *Regenerate key* operation applied to the keys: - *Ticket key* - *Configuration key* - *Audit key* *Regenerate key* operation only can be executed in maintenance mode.
FDP_ITC.1 Import of user data without security attributes	During the *Regenerate key* operation, the Administrator shall enter the key passphrase that protects the *Configuration's key* inside the SSH's console.
FDP_ACC.1/Management Subset access control for *Regenerate key* operation applied to *database key* FDP_ACF.1/Management Security attribute based access control for *Regenerate key* operation applied to *database key*	The TOE controls the access to *Regenerate key* operation applied to the *Database key*. *Regenerate key* operation only can be executed in maintenance mode.

SFRs related to key regeneration	
FDP_ITC.2 Import of user data with security attributes	The *Regenerate key* applied to *Database key* starts a process that imports all policies from database to be resigned with the new key. This import operation verifies the integrity of each policy.
FDP_ETC.1 Export of user data without security attributes	During the regeneration of database key, the TOE generates the hash of the policy and sends to the HSM to sign with the new database Key.
FDP_ITC.2 Import of user data with security attributes FPT_TDC.1 Inter-TSF basic TSF data consistency FMT_MSA.1/Key-Regen Management of security attributes FDP_ETC.2 Export of user data with security attributes	During the regeneration of database key, the TOE retrieves the signature of signed policies. Then the TOE verifies the signature with the new database public key. Once the policy have the new integrity value verified, then the TOE saves the policy to database.

Table 31: SFRs related to key regeneration

6.6. Backup and restore (TSF.Backup)

The vinCERTcore provides backup and recovery functionalities in order to allow the reconstruction of the system in the event of a system failure, data loss or other serious error.

With that purpose, the TOE's interfaces can be used by an Operator or Administrator to backup and restore the following data:

- TOE configuration files
- Other information relevant for the recovery of the vinCERTcore system.

The integrity of the backup data is assured through the usage of digital signature. Regarding the protection of critical security parameters and other confidential information, it is ensured using encryption.

Additionally, the information kept on the database can reach hundreds of gigabytes, vinCERTcore database should be backed up using appropriate and databases specific tools, taking advantage of the partitioning and security mechanisms they support.

Also, the cryptographic material stored in HSM should be backed up using appropriate HSM tools of HSM's supplier.

Finally, the TOE's interfaces may also be used by the Auditor to backup audit log entries.

6.6.1. Backup and restore access control

Backup and restore operations are protected by the following access controls:

SFRs related to backup and restore access control	
FDP_ACC.1/Management Subset access control for *Generate backup* operation FDP_ACF.1/Management Security attribute based access control for *Generate backup* operation	The TOE controls and limits the access to generate the backup operation to Users with Administrator or Operator role. The TOE verifies the user account status and its role before processing the backup operation.
FDP_ACC.1/Management Subset access control for *Restore system* operation FDP_ACF.1/Management Security attribute based access control for *Restore system* operation	The TOE controls the access to restore system operation to Users with role Administrator or Operator. The TOE verifies the user account status and its role before processing the restore system operation.

Table 32: SFRs related to backup and restore access control

6.6.2. Backup generation

After backup file is generated, it must be exported to an external media (folder mapped in TOE's OS):

SFRs related to backup generation	
FDP_ETC.2 Export of user data with security attributes in *Generate Backup* operation	The TOE exports the backup file after backup file is properly encrypted and signed.

Table 33: SFRs related to backup generation

6.6.3. Restore system

The restore system operation restores the configuration of the TOE.

SFRs related to restore system	
FDP_ROL.1 Basic rollback	The TOE can execute rollback from backup file saved previously with backup generation.
FDP_ITC.2 Import of user data with security attributes	The TOE retrieves the backup archive from external media verifying its integrity and confidentiality.
FPT_TDC.1 Inter-TSF basic TSF data consistency	The TOE verifies backup archive integrity verifying its signature with infrastructure key. Once integrity is checked, backup file is deciphered.
FDP_UIT.1/Backup-archive Data exchange integrity	With signature in backup archive, the TOE can detect illegal modifications in backup file.

Table 34: SFRs related to restore system

6.7. Secure communications and session management (TSF.Comm)

Communication between the TOE and external components/systems follows the next:

- **TOE ↔ HSM:** This type of communication should be protected using the equipment's security mechanisms.
- **TOE ↔ Active Directory:** This communication is secured using Lightweight Directory Access Protocol Secure (LDAPS) using TLS communication.
- **TOE ↔ Database:** Since the database is installed in the same machine, there is no need to adopt specific controls to protect the connection with it. However, whenever possible, advantage should be taken of the database's security mechanisms (e.g. encrypted channel supported by MySQL and PostgreSQL).
- **TOE ↔ PKI *(vinCERTcamgr)*:** This communication is secured using Secure Hypertext Transfer Protocol Secure (HTTPS) using TLS communication.
- **TOE ↔ Mail Server:** This communication is secured using Simple Mail Transfer Protocol Secure (SMTPS) using TLS communication.

SFRs related to secure communications	
FTA_SSL.3 TSF-initiated termination	The TOE controls the user session expending tickets with caducity. Once one user presents an expired ticket to process one operation the session is considered expired.
FTA_SSL.4 User-initiated termination	The user can request a log-off operation. When this operation is requested, the current session ticket is stored in TOE internal cache during token time life. If the same user requests access to TSFs with this ticket, the system recognizes that as an invalid ticket.
FTP_ITC.1 Inter-TSF trusted channel	The TOE consumes the following services verifying the integrity of the connection: - *Active Directory Server (based on ldap protocol)* - *Database* - *PKI (vinCERTcamgr)* - *Mail Server* The TOE uses the official *HSM SDK* to connect to *HSM*. This type of communication should be protected using the equipment's security mechanisms.
FTA_TSE.1 TOE session establishment	*SSH-Client* and *vinCERTweb* client connects to the TOE using secure connection. The connection is protected using a secure SSL channel.

SFRs related to secure communications	
FTP_ITC.1 Inter-TSF trusted channel for *External-media communication*	The TOE uses a directory from TOE operating system to export the audit archive data. Additionally the TOE uses a folder in operating system to import and export system backup in operations generate backup and restore system. Since the filesystem is in the same machine, there is no need to adopt specific controls to protect the connection with it.
FTA_TSE.1 TOE session establishment *for vinCERTagent communication*	The main communication between *vinCERTagent* client and the TSF is always secure. This communication is implemented using the TLS [12] protocol. This secure communication guarantees the secrecy and data integrity of the messages to and from the TOE as well as the authentication of the TOE to the external application, which is based on the TLS protocol.

Table 35: SFRs related to secure communications

6.8. Secure start-up and self-test (TSF.Start)

During the TOE's start-up, the system performs the following set of verifications performed in two steps:

- *Start-up verifications*: This set of verifications applies when the TOE starts.
- *Connection verifications*: This set of verifications applies when the TOE have a valid configuration data loaded.

SFRs related to start-up and self-test	
FPT_TST.1 TSF testing	The TOE processes the following *Start-up verifications*: - Test integrity of executable code by verifying its digital signature - Test integrity and confidentiality of configuration file verifying its digital signature and decrypting data. Once the configuration is retrieved, the TOE processes the *Connection verifications* to the environment elements: - *Database connection* - *Active directory connection* - *PKI (vinCERTcamgr) connection* - *SMTPS connection*
FDP_ETC.1 Export of user data without security attributes	During the start-up the TOE sends the *cyphered configuration* to the HSM to decrypt its data.
FDP_ITC.2 Import of user data with security attributes	The TOE retrieves the configuration data deciphered inside the HSM.
FPT_TDC.1 Inter-TSF basic TSF data consistency	Finally, the TOE verifies the integrity of configuration data by verifying its digital signature.

Table 36: SFRs related to start-up and self-test

7. References

[1] Common Criteria for information Technology Security Evaluation, *Part 1: Introduction and general model*, September 2012.

[2] Common Criteria for information Technology Security Evaluation, *Part 2: Security functional components*, September 2012.

[3] Common Criteria for information Technology Security Evaluation, *Part 3: Security assurance components*, September 2012.

[4] DIN CEN/TS 419241 DIN SPEC 91126, *Security Requirements for Trustworthy Systems supporting Server Signing*.

[5] European Parliament and of the Council, *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*.

[6] ETSI, *ETSI/TS 102 176, v2.0.0*, 2007.

[7] CWA 14170, *Security requirements for signature creation applications*, MAy 2004.

[8] National Institute of Standards and Technology, *FIPS 140-2*, May 2001.

[9] RSA Laboratories, *PKCS#5*, September 2000.

[10] RSA Laboratories, *RFC7292 - PKCS #12*, July 2014.

[11] R. Security, *RFC2986 - PKCS #10*, November 2000.

[12] RFC5246, *The Transport Layer Security (TLS) Protocol, Version 1.2*, August 2008.

[13] ETSI, *ETSI/TS 101 733, v1.7.3*, 2007.

Annex A. Terms, definitions and abbreviations

Advanced Electronic Signature
Electronic signature which meets the following requirements:

- it is uniquely linked to the signer;
- it is capable of identifying the signer;
- it is created using means that the signer can maintain under his sole control; and
- It is linked to the data to which it relates in such a manner that any subsequent alteration of the data is detectable.

[5]

Certificate
Electronic attestation that links a signature verification data to a person, and confirms the identity of that person
[5]

Certificate Identifier
Unambiguous identifier of a Certificate

Certification Service Provider
Entity or a legal or natural person who issues certificates or provides other services related to electronic signatures
[5]

Data Content Type
Signature attribute that expresses the encoding format of the Signers' Document (SD)

Data To Be Signed
Data (e.g. a document or parts of a document) to be signed as well as any signature attributes that are bound together with the data by the signature.

NOTE: Data To Be Signed is the input to the cryptographic signing algorithm. The specific way that Data To Be Signed and any signature attributes are fed as input is defined in the specifications of the signature type in use.

Electronic Signature
Data in electronic form attached to - or logically associated with - other electronic data and which serves as a method of authentication of that data.
[5]

Qualified Certificate
Certificate which meets the requirements laid down in Annex 1 of the Directive [i.e. Dir. 1999/93/EC] and is provided by a certification service provider who fulfils the requirements laid down in Annex 11 of that Directive.
[5]

Qualified Electronic Signature
Advanced electronic signature which is based on a qualified certificate and which is created by a secure signature creation device.
[5]

Secure Signature Creation Device
Signature creation device that meets the requirements laid down in Annex 111 of the EU Directive.
[5]

Signatory (signer).
Person who holds a signature creation device and acts either on his own behalf or on behalf of the natural or legal person he represents.
[5]
Note: The term 'signer' is used throughout this document as a synonym.

Server Signing Application
Application that provides a remote access to the Signature Creation Application (SCA)

Signature Creation Application
Application that creates an electronic signature, using the digital signature produced by an SCDev connected to the SCA

Signature Creation Data
Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature
[5]

Signature Creation Data Identifier
Unambiguous identifier of a SCD

Signature Creation Device
Configured software or hardware used to implement the SCD
[5]
Note: Secure Signature Creation Device (SSCD) or Hardware Security Module (HSM) are examples of Signature Creation Devices (SCDev).

Signature Creation Environment
Physical, geographical and computational environment of the signature creation system

Signature Generation Service Provider
Trust Service provider which provides trust services that allow secure remote management of signatory's signature creation device and generation of electronic signatures by means of such a remotely managed device

Signature Invocation
Non-trivial interaction between the signer and the SSA or SCDev that is necessary to invoke the start of the signing process in the SSA/SCDev to generate the Signed Data Object (SDO), and that is the 'Wilful Act' of the signer

Signature Policy
Set of rules for the creation and validation of an electronic signature, that defines the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need, and under which the signature can be determined to be valid.
[13] ETSI/TS 101 733

Signature Suite
Combination of a signature algorithm with its parameters, a key generation algorithm, a padding method, and a cryptographic hash function [6] ETSI/TS 102 176

Signed Data Object (s)
Document(s) or parts of the document(s) for which an electronic signature has been generated, along with the electronic signature

Signer's Activation Data
Data (e.g. PIN, password or biometric data, one time password or cryptographically generated authentication token) which is used to authenticate the signer to the SCDev and which is required to allow the use of the SCD held on the SCDev and which may be referred to as 'Activation Data' in other documents

Signer's/Signers' Document
Document for which one or more signers intend to create an Electronic Signature or for which an Electronic Signature was created

Trusted Path
Path between two entities or components within an SSA that provides integrity and authenticity

Trust Service Provider
Entity which provides electronic services which enhances trust and confidence in electronic transactions

Trustworthy System Supporting Server Signing (TW4S)
Server-side system using SCD in order to create Advanced Electronic Signatures (AdES) in accordance with the requirements of the European Directive on Electronic Signatures
Note: The system includes at least an SSA and a SCDev.