REF: 2013-31-INF-1370 v2	Created by: CERT8
Target: Expediente	Revised by: CALIDAD
Date: 02.10.2014	Approved by: TECNICO

CERTIFICATION REPORT

File: 2013-31 KEYONE CA 4.0

Applicant: A61930046 SAFELAYER SECURE COMMUNICATIONS

References:

[EXT-2339] Certification Request.

[EXT-2578] Evaluation Technical Report v2.2.

The product documentation referenced in the above documents.

Certification report of the product KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02), as requested in [EXT-2339] dated 07/11/2013, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-2578] received on 02/09/2014.

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02).

KeyOne CA is a software application that performs the Certification Authority functions of issuing public key digital certificates using the syntax defined in ITU-T X.509v3. KeyOne CA forms part of the Safelayer Public Key Infrastructure (PKI) solution. KeyOne CA can act as a Root CA, Subordinate CA, Cross CA, Bridge CA, Online CA and Offline CA. Depending on how it is used, the CA operates in conjunction with a Registration Authority product that assumes the entity registration functions. KeyOne CA can also operate in conjunction with the Validation Authority product to provide the digital certificate validation service. The main functions of KeyOne CA are to:

- Generate and protect the private keys via the use of cryptographic devices (HSM).
- Automatically manage the life-cycle and the coexistence of the private keys of the CA.
- Manage recognized RAs and assign them certification policies.
- Generate the ITU-T X509v3 digital certificates (for users and applications) requested by the RAs.
- Generate and publish lists of revoked and suspended digital certificates (CRLs).
- Report on the status of the digital certificates so the validation service (VA) can publish it via OCSP.
- Guarantee the secure auditing of the events and actions carried out in the system.

KeyOne CA is designed to facilitate compliance with the security requirements for trustworthy systems managing certificates for electronic signatures (CEN CWA 14167-1) in terms of roles and events. It facilitates adaptation to the ETSI TS 101 456 recommendations for certification authority policies that issue recognized digital certificates. The system support FIPS 140-2 level 3 HSMs.

KeyOne XRA is part of the Safelayer Public Key Infrastructure (PKI) solution. KeyOne XRA operates as a user/application registration service (RA) for requesting the issuing and revocation of digital certificates (in conjunction with KeyOne CA).

KeyOne XRA is extremely adaptable to business needs: for user registration processes and for the delivery of digital certificates to users. Its workflow manager provides simple and reliable system configuration for defining what data processing actions are to be included in the registration process and what data the system is to exchange with users, operators and applications.

The main functions of KeyOne XRA are to:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

- User registration and digital certificate life-cycle management through interaction with KeyOne CA.
- Certificate life-cycle management for PKI services and applications that require authentication, signature and data encryption.

KeyOne XRA includes the role management, auditing and reporting mechanisms recommended for digital certificate management systems for CEN CWA 14167-1 e-signature. It facilitates adaptation to the ETSI TS 101 456 recommendations for the policies of certification authority policies that issue recognized digital certificates. The system support FIPS 140-2 level 3 HSMs.

KeyOne VA is suitable for critical processes of electronic signature validation since it provides evidential value and greater efficiency in the verification of the status of the digital certificates (in contrast to the conventional mechanism which are based in revocation lists).

The main functions of KeyOne VA are to:

- Store information on the status of the certificates generated by one or more Certification Authorities. The status of a digital certificate is updated by downloading the revocation lists or the information provided by Certification Authorities (CA) that have the KeyOne publication service (KeyOne CertStatus Server) installed. In both cases, updating is performed remotely.
- Receive user or service-provider requests on the status of the digital certificates used in the signing of electronic transactions.
- Guarantee the non-repudiation of the responses. These responses are digitally-signed by the Validation Authority and specify the date and status (valid, revoked, cancelled or unknown) of a certificate.
- Generate event logs so operators can monitor the system status, its security and to what extent the corporate specifications are being met.

Customize the system to tailor response delivery and content to the identity of the requester. KeyOne products support defining the roles and events required to operate in compliance with the Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures (CWA14167-1). KeyOne VA supports the roles of security operator, system administrator and system auditor. The system support FIPS 140-2 level 3 HSMs.

Developer/manufacturer: Safelayer Secure Communications S.A.

Sponsor: Safelayer Secure Communications S.A.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Epoche & Espri S.L.U.

Protection Profile: “Certificate Issuing and Management Components Family of Protection Profiles” (CIMC) Security Level 3 Protection Profile, version 1.0, October 31, 2001, National Security Agency (NSA).

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Evaluation Level: EAL4+ (ALC_FLR.2).

Evaluation end date: 02/09/2014.

All the assurance components required by the evaluation level EAL 4 (augmented with ALC_FLR.2) have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL 4+ (ALC_FLR.2), as defined by the Common Criteria v3.1 R4 (CC_P1, CC_P2, CC_P3) and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02), a positive resolution is proposed.

TOE SUMMARY

The TOE is composed of the KeyOne CA (with the KeyOne CRLA and the KeyOne Passport Addins), the KeyOne VA and the KeyOne XRA products.

KeyOne CA is an application for creating and managing Certification Authorities of various types (root/subordinate, online/offline), allowing full management lifecycle of user certificates.

The purpose of KeyOne CA is to implement the functionality of a X.509 Certification Authority X.509 and implement the required functionality of the CV certificates Certification Authorities to establish the electronic passport.

In the KeyOne PKI, KeyOne CA implements the certificate management system. This application:

- Provides services of X.509 and CV certificates generation, to issue certificates to subscribers.
- Defines certification profiles that apply to requests for X.509 certificates and CV processed by the certificate generation service.
- Provides a service of X.509 certificate revocation, to process incoming requests for revocation that may result in suspension, revocation or rehabilitation of certificates of subscribers.
- Provides a CV certificates revocation, to process requests for revocation that result in the impossibility of automatically authenticate a subsequent certification request with the key of the revoked certificate.
- Provides a service to generate X.509 CRLs, in order to issue the certificate revocation lists that can be exported and published in repositories to be accessed by entities that are interested in checking the status of certificates of subscribers.
- Defines the X.509 CRLs profiles that set fields and extensions of the CRLs that will be issued.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

- Guarantees the secure auditing of the events and actions carried out in the system.

KeyOne CA implements public key certification functions (using the syntax defined in ITU-T Recommendation X.509 | ISO/IEC 9594-8 v3). These functions are accessible via:

- The graphical interface of the application.
- The SOAP/WS interface of the application server.
- Other KeyOne components, as the KeyOne XRA (that acts as the Registration Authority).

The functions of KeyOne CA can be extended with the KeyOne CRLA extension and a set of optional extensions for implementing electronic passport infrastructures.

In KeyOne, the generation of CRLs is implemented with the KeyOne CRLA extension for KeyOne CA. This extension periodically updates and generates CRLs that contain all the certificates revoked by a certification system at a point in time.

The electronic passport is divided into the following two components:

- The Extended Access Control (EAC) infrastructure for the second generation of e-Passports. In this case the passport is able to authenticate the reader using a PKI of CV certificates. Thus, the passport can restrict access from the data, depending on the access permissions contained in the certificate of the reader.
- The infrastructure for the first generation of electronic travel documents, which was standardized by the International Civil Aviation Organization (ICAO). In this case the data contained in the electronic passports are signed using a PKI of X.509 certificates. Thus the application that accesses this data can validate that it is a passport which data are integer (have been generated by a legitimate entity). Protection against cloning uses a system based on a challenge-response called Active Authentication (AA).

KeyOne XRA is an application for implementing all the registration functions. It:

- Registers the data of end entities.
- Generates certification requests for end entities.
- Sends the certificates to the owners and publishes them in the repositories.
- Generates certificate renewal and revocation requests.

These functions are accessible via the graphical interface of the application.

KeyOne VA is a system for electronic-signature verification critical processes. The main advantages of this system are:

- Proof of response delivery.
- Greater efficiency in validating certificate status.

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

The KeyOne VA validation service is based on the IETF OCSP. The system:

- Responds to the requests for information on the status of digital certificates used in the signing of electronic transactions. These requests may come from users or service providers.
- Stores information on the status of certificates generated by one or more Certification Authorities.
- Guarantees the non-repudiation of the responses. The responses include a digital signature from the Validation Authority that specifies the date and status (valid, revoked, suspended or unknown) of the certificate.

To do these things, KeyOne VA can operate with a HSM (network or internal) and requires access to a database and a network timesource.

The KeyOne Console is administration console enabling the user to graphically manage several common aspects of a KeyOne system, such as the:

- Users and roles.
- Access to external resources (e.g., data repositories, cryptographic hardware).
- Installation in multiple machines.
- Recording of events (logs).

The configuration performed through the KeyOne Console is applicable for all the TOE components.

The PKI systems implemented by the KeyOne products are run in a shared environment known as the KeyOne system kernel, or, more simply, the KeyOne system. KeyOne applications share an execution and administration environment.

The following picture describes the general architecture of the TOE.

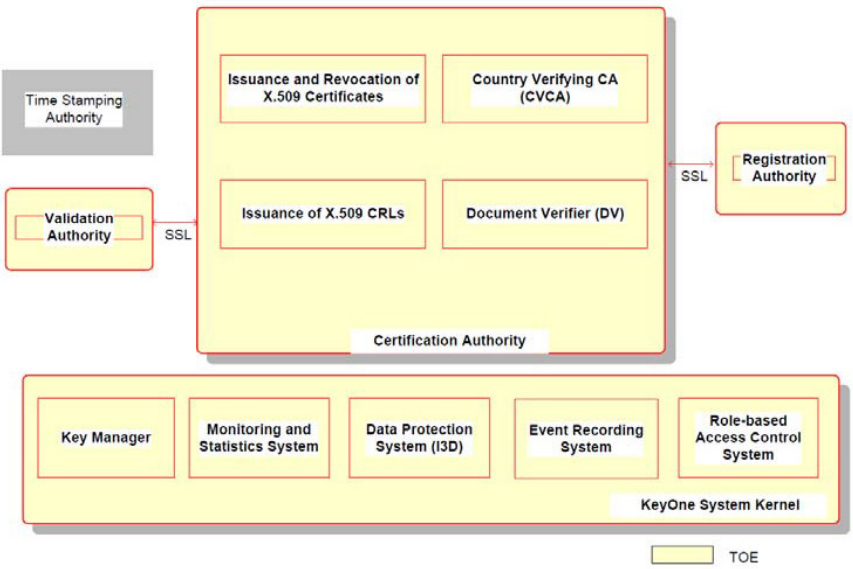


Figure 1 – TOE CA Architecture

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Using KeyOne CA it is possible to define the following three types of Certification Authorities:

- Generic X.509 Certification Authority
- Country Verifying CA (CVCA)
- Document Verifier (DV)

The following are the Product Logical Features and Functionality that are not included in the TOE and therefore they have not been evaluated:

- Additional command line scripts installed with the product (except i3dverify, i3dfix and i3dcompact which are part of the TOE and evaluated).
- Additional elements of the KeyOne solution:
  - CVRA
  - TSA
  - CertStatus-Addin

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL 4 and the evidences required by the additional component ALC_FLR.2, according to Common Criteria v3.1 R4 (CC_P1, CC_P2, CC_P3).

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.2 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: basic design
	ATE_FUN.1 Functional testing

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Assurance Class	Assurance components
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

The ST claims conformance to an old PP developed under version 2.1 of the CC. However, the ST claims conformance to the CC version 3.1 R4. The following SARs belonging to the CC v2.1 are included in "Certificate Issuing and Management Components Family of Protection Profiles" (CIMC) Security Level 3 Protection Profile, version 1.0, October 31, 2001, National Security Agency (NSA).

Assurance Class	Component ID	Component Title	EAL Level
Configuration Management	ACM_CAP.3	Authorization controls	EAL 3
	ACM_SCP.2	Problem tracking CM coverage	EAL 4
Delivery and Operation	ADO_DEL.2	Detection of modification	EAL 4 – 6
	ADO_IGS.1	Installation, generation, and start-up procedures	EAL 1 – 7
Development	ADV_FSP.2	Fully defined external interfaces	EAL 4
	ADV_HLD.2	Security enforcing high-level design	EAL 3 – 4
	ADV_IMP.1	Subset of the implementation of the TSF	EAL 4
	ADV_LLD.1	Descriptive low-level design	EAL 4 – 5
	ADV_RCR.1	Informal correspondence demonstration	EAL 1 – 4
	ADV_SPM.1	Informal TOE security policy model	EAL 4

Assurance Class	Component ID	Component Title	EAL Level
Guidance Documents	AGD_ADM.1	Administrator guidance	EAL 1 – 7
	AGD_USR.1	User guidance	EAL 1 – 7
Life Cycle Support	ALC_DVS.1	Identification of security measures	EAL 3 – 5
	ALC_FLR.2	Flaw reporting procedures	None
	ALC_TAT.1	Well-defined development tools	EAL 4
Tests	ATE_COV.2	Analysis of coverage	EAL 3 – 5
	ATE_DPT.1	Testing: high-level design	EAL 3 – 4
	ATE_FUN.1	Functional testing	EAL 2 – 5
	ATE_IND.2	Independent testing - sample	EAL 2 – 6
Vulnerability Assessment	AVA_MSU.2	Validation of analysis	EAL 4 - 5
	AVA_SOF.1	Strength of TOE security function evaluation	EAL 2 - 7
	AVA_VLA.2	Independent vulnerability analysis	EAL 4

As shown in the previous tables, at Security Level 3, the applicable CC assurance level is EAL3 augmented by selected requirements from EAL4. The majority of the requirements are from EAL3. An EAL3 evaluation provides an analysis supported by "gray box" testing, selective independent confirmation of the developer test results, and evidence of a developer search for obvious vulnerabilities. An EAL4 evaluation provides an analysis supported by the low-level design of the modules of the TOE,

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

and a subset of the implementation. Testing is supported by an independent search for obvious vulnerabilities.

The vendor, in its ST has claimed full EAL4, augmented by ALC_FLR.2 and has included all the associated SARs in its security target. According to the CCRA (see www.commoncriteriaportal.org/cc), "the member organisations of the CCRA declare that defined assurance levels (EALs) between versions of the criteria are equivalent and can therefore be used without restrictions for composition activities".

Therefore, the lab has considered correct the approach followed by the vendor including the CC v3.1 R4 SARs associated to EAL4+ (ALC_FLR.2) claiming also the conformance to the Protection Profile. The assurance activities declared and carried out by the lab, guarantee (when PASS) an equivalence or higher assurance than the one declared for the Protection Profile.

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4 (CC_P1, CC_P2, CC_P3):

Functional Requirements for the TOE lists all the functional security requirements for the TOE that are included in this Security Target. The requirements have been extracted from the CIMC Protection Profile. Some of these requirements have been instantiated by means the use of the operations mechanism offered by the Common Criteria standard. The following table lists all the security functional requirements for the TOE.

CLASS	FAMILY/COMPONENT	FUNCTIONAL REQUIREMENT
FAU	**GEN.1**	FAU_GEN.1.1
		FAU_GEN.1.2
	GEN.2	FAU_GEN.2.1
	SEL.1	FAU_SEL.1.1
	STG.1	FAU_STG.1.1
		FAU_STG.1.2
	STG.4	FAU_STG.4.1
FDP	**ACC.1**	FDP_ACC.1.1
	ACF.1	FDP_ACF.1.1
		FDP_ACF.1.2
		FDP_ACF.1.3

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

		FDP_ACF.1.4
	FDP_ACF_CIMC.2 User private key confidentiality protection	FDP_ACF_CIMC.2.1
		FDP_ACF_CIMC.2.2
	FDP_ACF_CIMC.3 User secret key confidentiality protection	FDP_ACF_CIMC.3.1
	FDP_SDI_CIMC.3 Stored public key integrity monitoring and action	FDP_SDI_CIMC.3.1
		FDP_SDI_CIMC.3.2
	FDP_ETC_CIMC.5 Extended user private and secret key export	FDP_ETC_CIMC.5.1
	FDP_CIMC_BKP.1 CIMC backup and recovery	FDP_CIMC_BKP.1.1
		FDP_CIMC_BKP.1.2
		FDP_CIMC_BKP.1.3
		FDP_CIMC_BKP.1.4
	FDP_CIMC_BKP.2 Extended CIMC backup and recovery	FDP_CIMC_BKP.2.1
		FDP_CIMC_BKP.2.2
	FDP_CIMC_CSE.1 Certificate status export	FDP_CIMC_CSE.1.1
	FDP_CIMC_CER.1 Certificate Generation	FDP_CIMC_CER.1.1
		FDP_CIMC_CER.1.2
		FDP_CIMC_CER.1.3
		FDP_CIMC_CER.1.4
	FDP_CIMC_OCSP.1 Basic Response Validation	FDP_CIMC_OCSP.1.1
	FDP_CIMC_CRL.1 Certificate Revocation	FDP_CIMC_CRL.1.1
	ITT.1 (iteration 1)	FDP_ITT.1.1 (FDP_ITT.1 iteration 1)
	ITT.1 (iteration 2)	FDP_ITT.1.1 (FDP_ITT.1 iteration 2)
	UCT.1	FDP_UCT.1.1
FIA	**UAU.1**	FIA_UAU.1.1

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

		FIA_UAU.1.2
	UID.1	FIA_UID.1.1
		FIA_UID.1.2
	ATD.1	FIA_ATD.1.1
	USB.1	FIA_USB.1.1
FPT	**FPT_CIMC_TSP.1 AUDIT LOG SIGNING EVENT**	FPT_CIMC_TSP.1.1
		FPT_CIMC_TSP.1.2
		FPT_CIMC_TSP.1.3
		FPT_CIMC_TSP.1.4
	ITC.1	FPT_ITC.1.1
	ITT.1 (ITERATION 1)	FPT_ITT.1.1 (FPT_ITT.1.1 ITERATION 1)
	ITT.1 (ITERATION 2)	FPT_ITT.1.1 (FPT_ITT.1.1 ITERATION 2)
	STM.1	FPT_STM.1.1
FMT	**FMT_MTD_CIMC.4 TSF PRIVATE KEY CONFIDENTIALITY PROTECTION**	FMT_MTD_CIMC.4.1
	FMT_MTD_CIMC.5 TSF SECRET KEY CONFIDENTIALITY PROTECTION	FMT_MTD_CIMC.5.1
	FMT_MTD_CIMC.7 EXTENDED TSF PRIVATE AND SECRET KEY EXPORT	FMT_MTD_CIMC.7.1
	FMT_MOF_CIMC.3 EXTENDED CERTIFICATE PROFILE MANAGEMENT	FMT_MOF_CIMC.3.1
		FMT_MOF_CIMC.3.2
		FMT_MOF_CIMC.3.3
		FMT_MOF_CIMC.3.4
	FMT_MOF_CIMC.5 EXTENDED CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	FMT_MOF_CIMC.5.1
		FMT_MOF_CIMC.5.2
		FMT_MOF_CIMC.5.3
	FMT_MOF_CIMC.6 OCSP PROFILE MANAGEMENT	FMT_MOF_CIMC.6.1
		FMT_MOF_CIMC.6.2

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

		FMT_MOF_CIMC.6.3
	MOF.1	FMT_MOF.1.1
	SMF.1	FMT_SMF.1.1
	MTD.1 (ITERATION 1)	FMT_MTD.1.1 (FMT_MTD.1 ITERATION 1)
	MTD.1 (ITERATION 2)	FMT_MTD.1.1 (FMT_MTD.1 ITERATION 2)
	SMR.1	FMT_SMR.1.1
	MSA.1 (ITERATION 1)	FMT_MSA.1.1 (FMT_MSA.1 ITERATION 1)
	MSA.1 (ITERATION 2)	FMT_MSA.1.1 (FMT_MSA.1 ITERATION 2)
	MSA.3	FMT_MSA.3.1
		FMT_MSA.3.2
FCS	**FCS_CKM_CIMC.5 CIMC PRIVATE AND SECRET KEY ZEROIZATION**	FCS_CKM_CIMC.5.1
FCO	**FCO_NRO_CIMC.3 ENFORCED PROOF OF ORIGIN AND VERIFICATION OF ORIGIN**	FCO_NRO_CIMC.3.1
		FCO_NRO_CIMC.3.2
		FCO_NRO_CIMC.3.3
	FCO_NRO_CIMC.4 ADVANCED VERIFICATION OF ORIGIN	FCO_NRO_CIMC.4.1
		FCO_NRO_CIMC.4.2

The security functional requirements that are applicable to the IT environment. All these requirements have been extracted from the [CIMC] Protection Profile, except the FMT_SMF.1.1 requirement (FMT_SMF Specification of Management Functions) that has been included in order to accomplish dependencies between functional requirements.

Some of these requirements have been instantiated by means the use of the operations mechanism offered by the Common Criteria. The following table lists all the security functional requirements for the IT environment, and the type of operation applied to them.

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

FUNCTIONAL REQUIREMENT	SECURITY TARGET OPERATION
FAU_GEN.1.1 (FAU_GEN.1 ITERATION 1)	SELECTION, ASSIGNMENT, REFINEMENT
FAU_GEN.1.2 (FAU_GEN.1 ITERATION 1)	REFINEMENT, ASSIGNMENT
FAU_GEN.2.1 (FAU_GEN.2 ITERATION 1)	REFINEMENT
FAU_SAR.1.1	ASSIGNMENT, REFINEMENT
FAU_SAR.1.2	REFINEMENT
FAU_SAR.3.1	SELECTION, ASSIGNMENT, REFINEMENT
FAU_SEL.1.1 (FAU_SEL.1 ITERATION 1)	SELECTION, ASSIGNMENT, REFINEMENT
FAU_STG.1.1 (FAU_STG.1 ITERATION 1)	REFINEMENT
FAU_STG.1.2 (FAU_STG.1 ITERATION 1)	SELECTION, REFINEMENT
FAU_STG.4.1 (FAU_STG.4 ITERATION 1)	SELECTION, ASSIGNMENT, REFINEMENT
FPT_STM.1.1 (FPT_STM.1 ITERATION 1)	REFINEMENT
FPT_SEP.1.1	REFINEMENT
FPT_SEP.1.2	REFINEMENT
FPT_RVM.1.1 (FPT_RVM.1 ITERATION 1)	REFINEMENT
FPT_ITC.1.1 (FPT_ITC.1 ITERATION 1)	REFINEMENT
FPT_ITT.1.1 (FPT_ITT.1 ITERATION 1)	SELECTION, REFINEMENT
FPT_ITT.1.1 (FPT_ITT.1 ITERATION 2)	SELECTION, REFINEMENT
FPT_AMT.1.1	SELECTION, REFINEMENT
FMT_SMR.2.1	ASSIGNMENT, REFINEMENT
FMT_SMR.2.2	REFINEMENT
FMT_SMR.2.3	ASSIGNMENT, REFINEMENT
FMT_MOF.1.1 (FMT_MOF.1 ITERATION 1)	SELECTION, ASSIGNMENT, REFINEMENT
FMT_MSA.1.1	SELECTION, ASSIGNMENT, REFINEMENT
FMT_MSA.2.1	REFINEMENT
FMT_MSA.3.1	SELECTION, ASSIGNMENT,

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

	REFINEMENT
FMT_MSA.3.2	ASSIGNMENT, REFINEMENT
FMT_MTD.1.1	ASSIGNMENT, SELECTION, REFINEMENT
FMT_SMF.1.1	ASSIGNMENT, REFINEMENT
FDP_ACC.1.1 (FDP_ACC.1 ITERATION 1)	ASSIGNMENT, REFINEMENT
FDP_ACF.1.1 (FDP_ACF.1 ITERATION 1)	ASSIGNMENT, REFINEMENT
FDP_ACF.1.2 (FDP_ACF.1 ITERATION 1)	ASSIGNMENT, REFINEMENT
FDP_ACF.1.3 (FDP_ACF.1 ITERATION 1)	ASSIGNMENT, REFINEMENT
FDP_ACF.1.4 (FDP_ACF.1 ITERATION 1)	ASSIGNMENT, REFINEMENT
FDP_ITT.1.1 (FDP_ITT.1 ITERATION 1)	ASSIGNMENT, SELECTIONN, REFINEMENT
FDP_ITT.1.1 (FDP_ITT.1 ITERATION 2)	ASSIGNMENT, SELECTIONN, REFINEMENT
FDP_UCT.1.1 (FDP_UCT.1 ITERATION 1)	ASSIGNMENT, SELECTION, REFINEMENT
FIA_ATD.1.1	ASSIGNMENT, REFINEMENT
FIA_UAU.1.1 (FIA_UAU.1 ITERATION 1)	ASSIGNMENT, REFINEMENT
FIA_UAU.1.2 (FIA_UAU.1 ITERATION 1)	REFINEMENT
FIA_UID.1.1 (FIA_UID.1 ITERATION 1)	ASSIGNMENT, REFINEMENT
FIA_UID.1.2 (FIA_UID.1 ITERATION 1)	REFINEMENT
FIA_USB.1.1 (FIA_USB.1 ITERATION 1)	REFINEMENT
FIA_AFL.1.1	REFINEMENT, SELECTION, ASSIGNMENT
FIA_AFL.1.2	ASSIGNMENT, REFINEMENT
FTP_TRP.1.1	SELECTION, REFINEMENT
FTP_TRP.1.2	SELECTION, REFINEMENT
FTP_TRP.1.3	ASSIGNMENT, SELECTION, REFINEMENT
FCS_CKM.1.1	ASSIGNMENT, REFINEMENT
FCS_CKM.4.1	ASSIGNMENT, REFINEMENT
FCS_COP.1.1	ASSIGNMENT, REFINEMENT

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

FPT_TST_CIMC.2.1	NONE
FPT_TST_CIMC.2.2	ASSIGNMENT
FPT_TST_CIMC.3.1	NONE
FPT_TST_CIMC.3.2	ASSIGNMENT

IDENTIFICATION

Product: KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02)

Security Target: Security Target – KeyOne 4.0 September, 2014 Document Identifier: 95A278AC v2.1.

Protection Profile: "Certificate Issuing and Management Components Family of Protection Profiles" (CIMC) Security Level 3 Protection Profile, version 1.0, October 31, 2001, National Security Agency (NSA).

Evaluation Level: Common Criteria v3.1 R4 (CC_P1, CC_P2, CC_P3) EAL4+ (ALC_FLR.2).

SECURITY POLICIES

The use of the product KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02) shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target. In short, it establishes the need of implementing organisational policies related to the following aspects.

Policy 01: P.Authorized use of information

Information shall be used only for its authorized purpose(s).

Policy 02: P.Cryptography

FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

Personnel

Assumption 01: A.Auditors Review Audit Logs

Audit logs are required for security-relevant events and must be reviewed by the Auditors.

Assumption 02: A.Authentication Data Management

An authentication data management policy is enforced to ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) (Note: this assumption is not applicable to biometric authentication data.)

Assumption 03: A.Competent Administrators, Operators, Officers and Auditors

Competent Administrators, Operators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.

Assumption 04: A.CPS

All Administrators, Operators, Officers, and Auditors are familiar with the Certificate Policy (CP) and Certification Practices Statement (CPS) under which the TOE is operated.

Assumption 05: A.Disposal of Authentication Data

Proper disposal of authentication data and associated privileges is performed after access has been removed (e.g., job termination, change in responsibility).

Assumption 06: A.Malicious Code Not Signed

Malicious code destined for the TOE is not signed by a trusted entity.

Assumption 07: A.Notify Authorities of Security Issues

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Administrators, Operators, Officers, Auditors, and other users notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.

Assumption 08: A.Social Engineering Training

General users, administrators, operators, officers and auditors are trained in techniques to thwart social engineering attacks.

Assumption 09: A.Cooperative Users

Users need to accomplish some task or group of tasks that require a secure IT environment. The users require access to at least some of the information managed by the TOE and are expected to act in a cooperative manner.

Connectivity

Assumption 10: A.Operating System

The operating system has been selected to provide the functions required by this Security Target to counter the perceived threats, as identified in this Security Target.

Physical

Assumption 11: A.Communications Protection

The system is adequately physically protected against loss of communications i.e., availability of communications.

Assumption 12: A.Physical Protection

The TOE hardware, software, and firmware critical to security policy enforcement will be protected from unauthorized physical modification.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02), although the agents implementing attacks have the attack potential according to the “Enhanced basic” of EAL4+ (ALC_FLR.2) and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Authorized Users

Threat 01: T.Administrative errors of omission

Administrators, Operators, Officers or Auditors fail to perform some function essential to security.

Threat 02: T.User abuses authorization to collect and/or send data

User abuses granted authorizations to improperly collect and/or send sensitive or security-critical data.

Threat 03: T.User error makes data inaccessible

User accidentally deletes user data rendering user data inaccessible.

Threat 04: T.Administrators, Operators, Officers and Auditors commit errors or hostile actions

An Administrator, Operator, Officer or Auditor commits errors that change the intended security policy of the system or application or maliciously modify the system's configuration to allow security violations to occur.

System

Threat 05: T.Critical system component fails

Failure of one or more system components results in the loss of system critical functionality.

Threat 06: T.Malicious code exploitation

An authorized user, IT system, or hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets.

Threat 07: T.Message content modification

A hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient.

Threat 08: T.Flawed code

A system or applications developer delivers code that does not perform according to specifications or contains security flaws.

Cryptography

Threat 09: T.Disclosure of private and secret keys

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

A private or secret key is improperly disclosed.

Threat 10: T.Modification of private/secret keys

A hacker modifies a secret/private key.

Threat 11: T.Sender denies sending information

The sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

External Attacks

Threat 12: T.Hacker gains access

A hacker masquerades as an authorized user to perform operations that will be attributed to the authorized user or a system process or gains undetected access to a system due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

Threat 13: T.Hacker physical access

A hacker physically interacts with the system to exploit vulnerabilities in the physical environment, resulting in arbitrary security compromises.

Threat 14: T.Social engineering

A hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

Non-IT security Objectives for the Environment

Environment objective 01: O.Administrators, Operators, Officers and Auditors guidance documentation

Deter Administrator, Operator, Officer or Auditor errors by providing adequate documentation on securely configuring and operating the environment.

Environment objective 02: O.Auditors Review Audit Logs

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Identify and monitor security-relevant events by requiring auditors to review audit logs on a frequency sufficient to address level of risk.

Environment objective 03: O.Authentication Data Management

Ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) through enforced authentication data management (Note: this objective is not applicable to biometric authentication data.)

Environment objective 04: O.Communications Protection

Protect the system against a physical attack on the communications capability by providing adequate physical security.

Environment objective 05: O.Competent Administrators, Operators, Officers and Auditors

Provide capable management of the TOE by assigning competent Administrators, Operators, Officers and Auditors to manage the TOE and the security of the information it contains.

Environment objective 06: O.CPS

All Administrators, Operators, Officers and Auditors shall be familiar with the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.

Environment objective 07: O.Disposal of Authentication Data

Provide proper disposal of authentication data and associated privileges after access has been removed (e.g., job termination, change in responsibility).

Environment objective 08: O.Installation

Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

Environment objective 09: O.Malicious Code Not Signed

Protect the TOE from malicious code by ensuring all code is signed by a trusted entity prior to loading it into the system.

Environment objective 10: O.Notify Authorities of Security Issues

Notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.

Environment objective 11: O.Physical Protection

Those responsible for the TOE must ensure that the security-relevant components of the TOE are protected from physical attack that might compromise IT security.

Environment objective 12: O.Social Engineering Training

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Provide training for general users, Administrators, Operators, Officers and Auditors in techniques to thwart social engineering attacks.

Environment objective 13: O.Cooperative Users

Ensure that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE.

Environment objective14: O.Lifecycle security

Provide tools and techniques used during the development phase to ensure security is designed into the environment. Detect and resolve flaws during the operational phase.

Environment objective 15: O.Repair identified security flaws

The vendor repairs security flaws that have been identified by a user.

IT Security Objectives for the Environment

Environment objective16: O.Cryptographic functions

The IT environment must implement approved cryptographic algorithms for encryption/decryption, authentication, and signature generation/verification; approved key generation techniques and use validated cryptographic modules (Validated is defined as FIPS 140-2 validated).

Environment objective 17: O.Operating System

The operating system used is validated to provide adequate security, including domain separation and non-bypassability, in accordance with security requirements recommended by the National Institute of Standards and Technology.

Environment objective 18: O.Periodically check integrity

Provide periodic integrity checks on both system and software.

Environment objective 19: O.Security roles

Maintain security-relevant roles and the association of users with those roles.

Environment objective 20: O.Validation of security function

Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.

Environment objective 21: O.Trusted Path

Provide a trusted path between the user and the system. Provide a trusted path to security-relevant (TSF) data in which both end points have assured identities.

Security Objectives for both the TOE and the Environment

Environment objective 22: O.Configuration Management

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Implement configuration management to assure identification of system connectivity (software, hardware, and firmware), and components (software, hardware, and firmware), auditing of configuration data, and controlling changes to configuration items.

Environment objective 23: O.Data import/export

Protect data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.

Environment objective 24: O.Detect modifications of firmware, software, and backup data

Provide integrity protection to detect modifications to firmware, software, and backup data.

Environment objective 25: O.Individual accountability and audit records

Provide individual accountability for audited events. Record in audit records: date and time of action and the entity responsible for the action.

Environment objective 26: O.Integrity protection of user data and software

Provide appropriate integrity protection for user data and software.

Environment objective 27: O.Limitation of administrative access

Design administrative functions so that Administrators, Operators, Officers and Auditors do not automatically have access to user objects, except for necessary exceptions. Control access to the system by Operators and Administrators who troubleshoot the system and perform system updates.

Environment objective 28: O.Maintain user attributes

Maintain a set of security attributes (which may include role membership. access privileges, etc.) associated with individual users. This is in addition to user identity.

Environment objective 29: O.Manage behavior of security functions

Provide management functions to configure, operate, and maintain the security mechanisms.

Environment objective 30: O.Object and data recovery free from malicious code

Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code.

Environment objective 31: O.Procedures for preventing malicious code

Incorporate malicious code prevention procedures and mechanisms.

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Environment objective 32: O.Protect stored audit records

Protect audit records against unauthorized access, modification, or deletion to ensure accountability of user actions.

Environment objective 33: O.Protect user and TSF data during internal transfer

Ensure the integrity of user and TSF data transferred internally within the system.

Environment objective 34: O.Require inspection for downloads

Require inspection for downloads

Environment objective 35: O.Respond to possible loss of stored audit records

Respond to possible loss of audit records when audit trail storage is full or nearly full by restricting auditable events.

Environment objective 36: O.Restrict actions before authentication

Restrict the actions a user may perform before the TOE authenticates the identity of the user.

Environment objective 37: O.Security-relevant configuration management

Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.

Environment objective 38: O.Time stamps

Provide time stamps to ensure that the sequencing of events can be verified.

Environment objective 39: O.User authorization management

Manage and update user authorization and privilege data to ensure they are consistent with organizational security and personnel policies.

Environment objective 40: O.React to detected attacks

Implement automated notification (or other responses) to the TSF-discovered attacks in an effort to identify attacks and to create an attack deterrent.

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

ARCHITECTURE

The PKI systems implemented by the KeyOne products are run in a shared environment known as the KeyOne system kernel, or, more simply, the KeyOne system. KeyOne applications share an execution and administration environment.

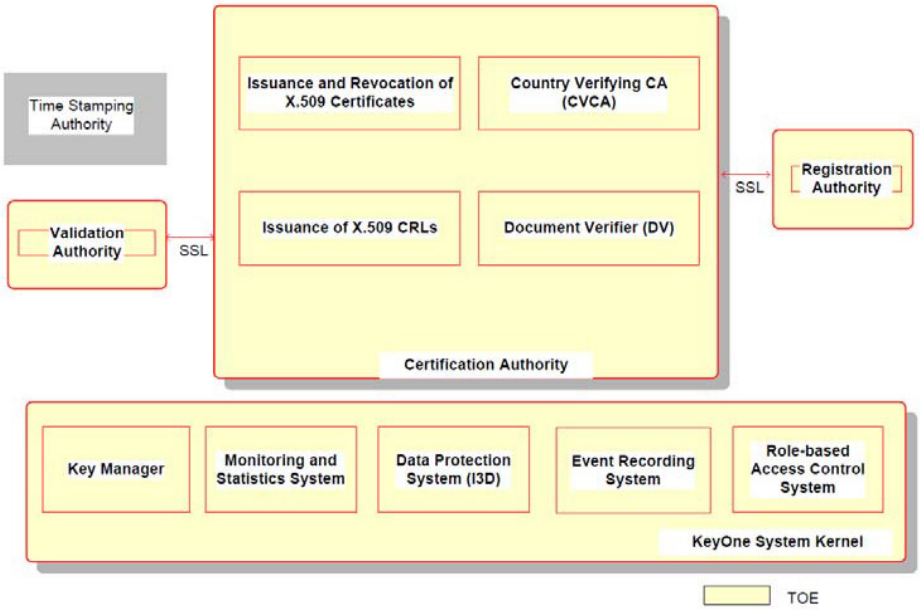


Figure 2. KeyOne CA Architecture

Using KeyOne CA it is possible to define the following three types of Certification Authorities:

Generic X.509 Certification Authority

X.509 Certification Authority that allows the issuance of X.509 certificates and CRLs. Depending on your settings can be a root or subordinate CA, and can provide its certification services online or offline through user interfaces that can be accessed by an operator.

Subscribers are individuals or entities to which the CA issues certificates. These subscribers can not access directly to services offered by KeyOne CA. Only the KeyOne CA operators can process certification or revocation requests through the user interface.

KeyOne CA allows online access to the interface of issuance and revocation of certificates to the approved Registration Authorities (RA). KeyOne XRA is a axample of Registration Authority that access to the online service.

An example of CA that can be implemented using KeyOne CA is the root Certification Authority needed in the BAC electronic passport, called Country Signing

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Certification Authority (CSCA). In this case the Document Signer, that is the entity who signs the data contained in the passports, are the subscriptors of this CA.

Country Verifying CA (CVCA)

CV Root Certification Authority of the EAC ePassport. Each country creates its own CVCA, ie a hierarchy of CV certificates are generated by country. The CVCA of a country must issue certificates to all countries wishing to certify their passport readers so they can electronically access the data of their passports.

Entities to which the CA issues the certificates can not directly access to the CA services. Are the CA operators which can process certification and revocation requests through the CA user interface.

KeyOne CA allows online access to the interface of issuing certificates to the authorized Registration Authorities (RA). The KeyOne CVRA is an example of RA of this type of CA.

Document Verifier (DV)

CV subordinated Certification Authority of the EAC ePassport. This CA is certified by all countries, having to manage multiple sets of keys and the corresponding certificates, one for each country to which service.

This type of CA generates certificates for the electronic passport readers, which are managed by entities called Inspection System (IS). The passport reader must provide the certificate of the hierarchy of the country where the passport was issued, and therefore it must manage as many certificates as countries manage the DV.

Are the CA operators who can process certification and revocation requests, of the inspection systems through the CA graphical interface.

Inspection systems can access online to the CA interface of issuance of certificates.

To be able to automate the issue and renewal of certificates from the certification authority, an interface with the superior RA in the hierarchy, the Single Point of Contact (SPOC), is defined. The SPOC can communicate with all the CVCAs of all the countries for processing the certification requests from the DV. Because certificate issue time is indefinite, as, depending on the certificate request, foreign CVCAs must be contacted, communication is asynchronous and KeyOne CA provides an online interface for the SPOC to send the certificates when they are available.

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

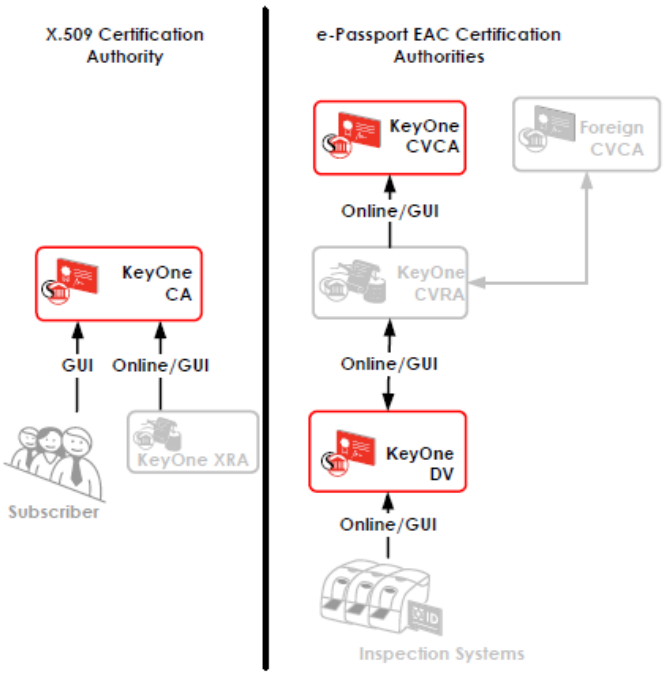


Figure 3. Types of Certification Authorities

Validation Authority (VA)

The VA issues evidences that certify the validity of digital certificates. To generate these evidences, a VA can access two complementary sources of information:

• A CA certification status service

• Certificate revocation lists.

Registration Authority (RA)

The registration authority interacts with the subscribers. It compiles and verifies the data contained in the certification and/or renewal requests.

The basic data structure for exchanges between KeyOne CA and the authorized RAs is a KeyOne batch. The RA generates a batch with certification/renewal requests that is processed in KeyOne CA in which, in the case of certification requests, a response batch is generated with the certificates created, or, for renewal requests, the change of status of the certificates is confirmed.

The RA can contact an administrator (one with privileges for processing KeyOne batches) and request the processing of the batch in the user interface or directly send the batch to the online batch processing service for an immediate response

External Entities:

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

Hardware Security Module (HSM)

To be able to provide its services, KeyOne CA must hold a set of keys, known as the service keys, along with their corresponding certificates. Both these service keys (CRL and certificate signature keys) and the infrastructure keys (batch signing, database integrity, sensitive data encryption, protection of online communications with external systems) are held in the HSM. The HSM performs all the cryptographic operations performed with the service and infrastructure keys.

To protect these keys, the system operator role is defined. Normally, M of a total of N operators are required for enabling access to these keys. Accessing these keys is required for starting the services in the KeyOne CA user interface.

In security terms, service keys are high-risk keys, and should therefore be stored in a FIPS 140-2 level 3 certified HSM (this is required if the system is configured for using a CIMC security policy).

Database Server

The database server is the relational database where KeyOne stores its configuration and the production data.

KeyOne takes advantage of the transactional properties of the databases to assure the atomicity of the changes made to the data when a function is processed.

Cryptographic Device for Authenticating in the User Interface

All KeyOne administrators require a key pair with its associated certificate for authenticating when accessing KeyOne applications. As these are lower risk keys tan the service keys, they can be stored on cryptographic tokens (although an HSM can be used).

Administrators must authenticate with their cryptographic devices to access the functions offered by the KeyOne user interface.

The cryptographic device is used for performing cryptographic operations for authenticating administrator.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- KeyOne 4.0 - Considerations for a Secure Operation. Document code: A5C273C9. Version 1.14. (08-Jul-2014).
- Product Installation and Uninstallation. Document code: A98558AB. Version 1.46 (05-Sep-2014).
- User Manual. Document Code: 8B4B9CFE. Version 1.61.
- KeyOne Console 4.0 Administration and Use. Document code: 3999D586. Version 2.3.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.
During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02) it is necessary the disposition of the following software components:

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

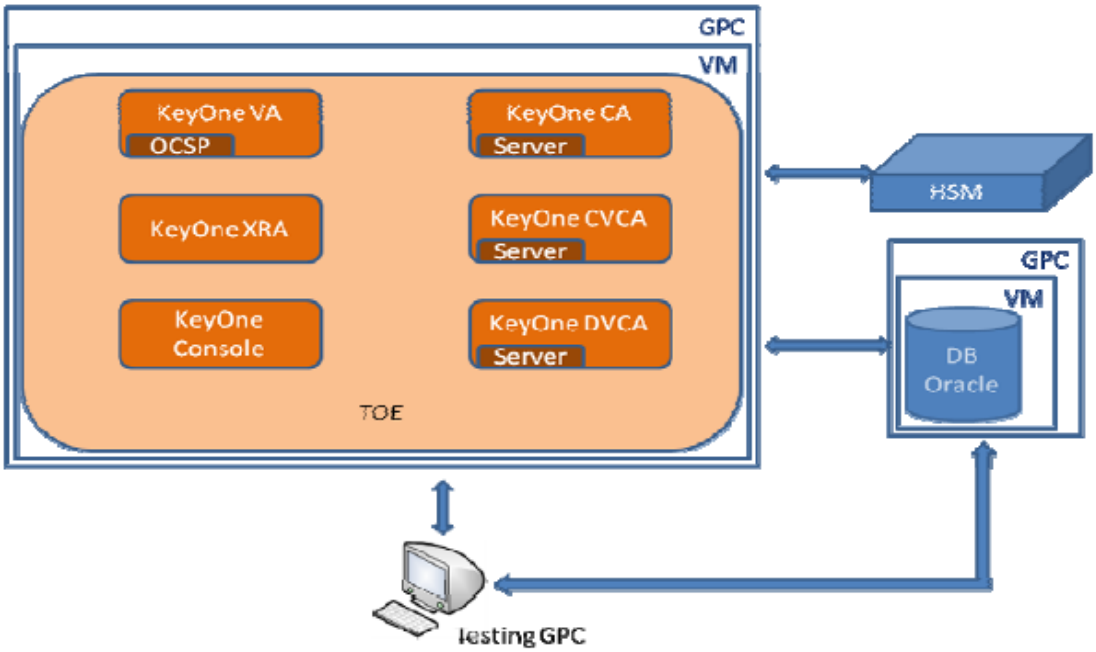
- Operating System: Windows Server 2012.
- Databases: Oracle 11g R2, Microsoft SQL Server 2012 Enterprise Edition SP1.
- Hardware Security Module: nCipher nShield Connect 1500, Safenet Luna SA 5.1.1 (FIPS 140-2 level 3).
- Java Runtime: JRE 1.7.0.
- Certificate-based PKI USB authenticator: Safenet eToken 510x.

The TOE configuration used to execute the functional tests and depth testing is consistent with the evaluated configuration according to the security target.

The evaluator has defined the test cases taking into account the security requirements defined in the security target and the described configuration (CIMC policy).

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

The following picture describes the operational environment used during the evaluation.



The evaluator has accessed the TOE by directly connecting to the GPC where the TOE is installed.

The evaluator has also used a GPC connected to the TOE network in order to access the online services of the TOE.

The connection between the GPC of the TOE, the GPC containing the database and the HSM is performed using an Ethernet network.

The evaluator has used the following tools in order to execute some test cases stated in this testing report:

- Wireshark v1.10.5 This tool has been used to capture and analyze network interface packets.
- Dream coder for Oracle v6.0 (build 6.0.2.0). This tool has been used to access and manage the TOE database.
- Openssl v1.0.1. Software used to generate and manage certificate data.
- Python interpreter v2.7.3. This interpreter has been used to run certain python scripts used in some tests. The following python libraries are needed:
  - Python-suds v0.4.1
  - httplib2 v 0.7.2
  - pycurl v 7.19.0
- Scripts developed by the evaluator.

The virtual machines are installed over VMWare Player v5.0.1 running in two GPC with Windows 7 Ultimate (64 bits) operating system.

The testing PC is a GPC using Windows 7 Ultimate (64 bits) operating system.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

The following are the Product Logical Features and Functionality that are not included in the TOE and therefore they have not been evaluated:

- Additional command line scripts installed with the product (except i3dverify, i3dfix and i3dcompact which are part of the TOE and evaluated).
- Additional elements of the KeyOne solution:
  - CVRA
  - TSA
  - CertStatus-Addin

EVALUATION RESULTS

The product KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02) has been evaluated against the Security Target Security Target – KeyOne 4.0 September, 2014 Document Identifier: 95A278AC v2.1.

All the assurance components required by the evaluation level EAL4+ (ALC_FLR.2) have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4+ (ALC_FLR.2), as defined by the Common Criteria v3.1 R4 (CC_P1, CC_P2, CC_P3) and the CEM.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The TOE usage is recommended given that there are no exploitable vulnerabilities in its operational environment.

The following usage recommendations are given:

- The TOE makes use of a cryptographic token as element to store and retrieve the user credentials for identification and authentication. It is recommended to use a strong password (lower case, upper case, numbers and symbols) for the token protection, in order to avoid any brute force attack.

- The TOE provides online services to the users, using the SSL protocol with known certificates. The TOE does not accept the connection unless the user provides a proper certificate generated or trusted by the TOE. However, it is not indicated (in the user manuals) that the users should also verify the TOE

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

certificates as part of the SSL channel establishment. Without this verification no assurance about the authenticity of the other party can be provided.

- The access control in the servers applications does not maintain the user attributes up to date. These are refreshed periodically and each time the server application is (re)started. The user manuals clearly indicate that the TOE administrators are in charge of re-starting the servers applications each time a modification in the user permissions occurs.

- The guidance documentation includes the TOE installation and configuration. Along the documents the vendor includes some notes indicating that certain security configuration must be applied for the CC evaluation configuration. These notes shall be strongly considered and applied in the TOE operational environment. Any configuration not considering the depicted security notes may incur in unprotected configuration and may contain security flaws.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product KeyOne CA 4.0, KeyOne XRA 4.0, KeyOne VA 4.0 version 4.0.13S2R1 (Release Patches 4.0.13S2R1_B01, 4.0.13S2R1_B02), a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, July 2009.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: Security Target – KeyOne 4.0 September, 2014 Document Identifier: 95A278AC v2.1.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20 · 28023 Madrid (Spain)
Email: organismo.certificacion@cni.es