REF: 2004-2-INF-65 v1
Difussion: Público
Date: 20.01.2006

Created by: CERT3
Reviewed by: TECNICO
Approved by: JEFEAREA

CERTIFICATION REPORT

Dossier: 2004-2 KEY ONE 3.0

References:

EXT-18	Certification request, dated 09-07-2004
EXT-125	Evaluation Technical Report, dated 29-12-2005
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

Certification report of the of the KeyOne 3.0 product, a Public Key Infrastructure software solution, version 3.0, release 04S2R1 with patches 3.0_04S2R1_B01, 3.0_04S2R1_B02, 3.0_04S2R1_B03, 3.0_04S2R1_B04, 3.0_04S2R1_B05, 3.0_04S2R1_B06 and3.0_04S2R1_B07, as requested by [EXT-18], and evaluated by CESTI-INTA, as detailed in the Evaluation Technical Report [EXT-125], received on the 11th of January, 2006, and in compliance with [CCRA].

This is a courtesy translation of the Scheme documentation for the purposes of its shadow certification.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Index

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Executive Summary

This document is the Certification Report of the KeyOne 3.0 product, a Public Key Infrastructure software solution, version 3.0, release 04S2R1 with patches 3.0_04S2R1_B01, 3.0_04S2R1_B02, 3.0_04S2R1_B03, 3.0_04S2R1_B04, 3.0_04S2R1_B05, 3.0_04S2R1_B06 and3.0_04S2R1_B07.

Developer: Safelayer Secure Communications, S.A.

Sponsor: Safelayer Secure Communications, S.A.

Certification Body: National Cryptological Centre (CCN)

ITSEF: IT Security Evaluation Centre (CESTI), of the Technical Aerospace National Institute “Esteban Terradas”(INTA).

PP claims: [CIMC], Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.

Evaluation Level: EAL4+ (ALC_FLR.2)

Strength of Function: Basic

Evaluation Technical Rreport date: 2006-01-11

All the assurance components required by the level EAL4+ (augmented with ALC_FLR.2, SOF high) have been assigned a “PASS” verdict. Consequently, the laboratory (CESTI /INTA) assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4+ methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Considering the obtained evidences during the instruction of the certification request of the KeyOne 3.0 product, version: 3.0, release 04S2R1 with patches 3.0_04S2R1_B01, 3.0_04S2R1_B02, 3.0_04S2R1_B03, 3.0_04S2R1_B04, 3.0_04S2R1_B05, 3.0_04S2R1_B06 and3.0_04S2R1_B07, a positive resolution is proposed.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

TOE summary

The TOE, KeyOne 3.0 product, 3.0 or KTS (KeyOne Trusted System), is a Public Key Infrastructure software solution. The system consists of the following elements:

- KeyOne LRA. Lightweigh Registration Authority.
- KeyOne RA. Registration Authority.
- KeyOne CA. Certification Authority.
- KeyOne VA. Validation Authority.
- KeyOne TSA. Time Stamping Authority.

The TOE offers the following services:

Core services

- Registration Service: Verifies the identity and, if applicable, any specific attributes of a Subscriber. The results of this service are passed to the Certificate Generation Service.

- Certificate Generation Service: Creates and signs certificates based on the identity and other attributes of a Subscriber as verified by the Registration Service.

- Revocation Management Service: Processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the Revocation Status Service.

- Revocation Status Service: Provides certificate revocation status information to relying parties. This service is based on revocation status information that is updated at regular intervals.

TOE Additional Services

- Subscriber Device Provision Service: Prepares and provides a Signature Creation Device (SCD) to Subscribers.

- Time Stamp Service: A third party, trusted to provide a Time Stamp Service.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

This table enumerates the services supported by the system, and relates them with the KeyOne subsystem where them resides.

Subsystem	**Services**
KeyOne LRA	Registration Service Subscriber Device Provision Service
KeyOne RA	Registration Service
KeyOne CA	Certificate Generation Service Revocation Management Service
KeyOne VA	Revocation Status Service
KeyOne TSA	Time Stamping Service

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfill EAL4, augmented with the component ALC_FLR.2.

Assurance Class	**Assurance Component**
Configuration Management	ACM AUT.1, ACM CAP.4, ACM SCP.2
Delivery and Operation	ADO DEL.2, ADO IGS.1
Development	ADV_FSP.2, ADV_HLD.2, ADV_IMP.1, ADV_LLD.1, ADV_RCR.1, ADV_SPM.1
Guidance	AGD ADM.1, AGD USR.1
Life Cycle	ALC DVS.1, ALC LCD.1, ALC FLR.2, ALC TAT.1
Tests	ATE COV.2, ATE FUN.1, ATE IND.2, ATE DPT.1
Vulnerability Analysis	AVA SOF.1, AVA VLA.2, AVA MSU.2

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Security Functional Requirements

The product security functionality satisfies, with the support from the environment, the [CIMC], Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003, protection profile.

The functional requirements satisfied by the product are:

Requirements expressed as of [CC_P2]:

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SEL.1 Selective Audit
- FAU_STG.1 Protected audit trail storage
- FAU_STG.4 Prevention of audit data loss
- FPT_STM.1 Reliable time stamps
- FMT_MOF.1 Management of security functions behavior
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access
- FDP_ITT.1 Basic internal transfer protection
- FDP_UCT.1 Basic data exchange confidentiality
- FPT_RVM.1 Non-bypassability of the TSP
- FPT_ITC.1 Inter-TSF confidentiality during transmission
- FPT_ITT.1 Basic internal TSF data transfer protection
- FIA_UAU.1 Timing of authentication
- FIA_UID.1 Timing of identification
- FIA_USB.1 User-subject binding

Requirements augmented by [CIMC]:

- FPT_CIMC_TSP.1 Audit log signing event
- FDP_ACF_CIMC.2 User private key
- FDP_ACF_CIMC.3 User secret key
- FDP_SDI_CIMC.3 Stored public key integrity monitoring and action
- FDP_ETC_CIMC.5 Extended user private and
- FDP_CIMC_BKP.1 CIMC backup and recovery
- FDP_CIMC_BKP.2 Extended CIMC backup and recovery
- FDP_CIMC_CSE.1 Certificate status export
- FDP_CIMC_CER.1 Certificate Generation
- FDP_CIMC_CRL.1 Certificate revocation list
- FDP_CIMC_OCSP.1 OCSP basic response
- FCO_NRO_CIMC.3 Enforced proof of origin and verification of origin
- FCO_NRO_CIMC.4 Advanced verification of origin
- FMT_MTD_CIMC.4 TSF private key confidentiality protection
- FMT_MTD_CIMC.5 TSF secret key confidentiality protection
- FMT_MTD_CIMC.7 Extended TSF private and secret key export

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

- FMT_MOF_CIMC.3 Extended certificate profile management
- FMT_MOF_CIMC.5 Extended certificate revocation list profile management
- FMT_MOF_CIMC.6 OCSP Profile Management
- FCS_CKM_CIMC.5 CIMC private and secret key

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Identification

Product: KeyOne 3.0 product, a Public Key Infrastructure software solution, version 3.0, release 04S2R1 with patches 3.0_04S2R1_B01, 3.0_04S2R1_B02, 3.0_04S2R1_B03, 3.0_04S2R1_B04, 3.0_04S2R1_B05, 3.0_04S2R1_B06 and3.0_04S2R1_B07.

Security Target: SECURITY TARGET KeyOne 3.0 (B4E6DBC0), 1.38.

PP claims: CIMC, Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.

Evaluation Level: EAL4+ (ALC_FLR.2)

Strength of Function: Basic

Evaluation Technical Report date: 2006-01-11

Security Policy

The TOE installation and operation must comply with the following security policies, as mandated in [CIMC]:

> **P.AUTHORIZED USE OF INFORMATION**
> Information shall be used only for its authorized purpose(s).
>
> **P.CRYPTOGRAPHY**
> FIPS-approved or NIST-recommended cryptographic functions shall be used to perform all cryptographic operations.

Assumptions and Clarification of Scope

Usage Assumptions

The usage assumptions are organized in three categories: personnel, physical and connectivity. The physical assumptions are detailed in the environmental assumptions section.

Personnel

Assumptions about administrators and users of the system as well as any threat agents.

> **A.Auditors Review Audit Logs**
> Audit logs are required for security-relevant events and must be reviewed by the Auditors.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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).

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.

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. This documentation is conformant with [NPKI] certificate policy.

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).

A.Malicious Code Not Signed
Malicious code destined for the TOE is not signed by a trusted entity.

A.Notify Authorities of Security Issues
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.

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

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.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Connectivity

Assumptions about other IT systems that are necessary for the secure operation of the TOE.

A.Operating System
The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats for the CIMC level 3 PP, as identified in this Security Target.

A.NTP Client
All the hosts included in the TOE have installed an NTP client that synchronises the system clock with a reliable clock that obtains the Coordinated Universal Time from a reliable source.

Environmental assumptions

Physical assumptions

Assumptions about the physical location of the TOE or any attached peripheral devices.

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

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

TOE Users

The intended users of the TOE services are classified in two main groups.

External Users
End User / Certificate Entity, is the subject of the certificate that binds its identity with its public key. There are other types of entities that can be certified, for example applications, servers.
Relying Parties, users or agents or any external trust services that rely on the data in a certificate in making decisions, following the verification processes and limitations established in the certificate policies for each type of certificates issued by KTS.
Auditing Entities, who require access to audit trails for conducting evaluation processes to review certificate practices.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Internal Users
PKI administrators, who can configure and administer the different applications supported by the TOE: Registration, Certificate Authority, Validation Authority, Time Stamping authority.
Registration Officer is responsible for the operation of the Lightweight Registration Authority and the Registration Authority, according to established registration procedures.

Suitable usage environments

The use of this TOE is more suitable to certain registry schemes. This configuration adapts perfectly to:

- Distributed register environments, due to the fast and easy deployment of different RAs, without increasing maintenance needs.
- Mobile or travelling registers, guaranteeing the security of the register service without very restrictive physical protections measures.

Clarification of scope

The following threats, organized in four categories (authorized users, system, cryptography, and external attacks) are covered by the TOE or by the environment or by both of them.

Authorized Users

T.Administrative errors of omission
Administrators, Operators, Officers or Auditors fail to perform some function essential to security.

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.

T.User error makes data inaccessible
User accidentally deletes user data rendering user data inaccessible.

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

T.Critical system component fails
Failure of one or more system components results in the loss of system critical functionality.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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.

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.

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

Cryptography

T.Disclosure of private and secret keys
A private or secret key is improperly disclosed.

T.Modification of private/secret keys
A secret/private key is modified.

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

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.

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

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

Any other threats not included in this section are NOT covered by the evaluated TOE, and no claim of resistance is made by the certification.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Security functional requirements for the TOE environment

The product requires the cooperation from its operational environment to fulfill the [CIMC], Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003, protection profile.

The security functional requirements that must be fulfilled by the TOE environment are the following:

Requirements expressed as of [CC_P2]:

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FAU_SAR.3 Selectable audit review
- FAU_SEL.1 Selective Audit
- FAU_STG.1 Protected audit trail storage
- FAU_STG.4 Prevention of audit data loss
- FPT_STM.1 Reliable time stamps
- FPT_SEP.1 TSF domain separation
- FPT_RVM.1 Non-bypassability of the TSP
- FPT_ITC.1 Inter-TSF confidentiality during transmission
- FPT_ITT.1 Basic internal TSF data transfer protection
- FPT_AMT.1 Abstract machine test
- FMT_SMR.2 Restrictions on security roles
- FMT_MOF.1 Management of security functions behavior
- FMT_MSA.1 Management of security attributes
- FMT_MSA.2 Secure security attributes
- FMT_MSA.3 Static attribute initialisation
- FMT_MTD.1 Management of TSF data
- FMT_SMF.1 Specification of Management Functions
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access
- FPT_ITT.1 Basic internal TSF data transfer protection
- FDP_UCT.1 Basic data exchange confidentiality
- FIA_ATD.1 User attribute definition
- FIA_UAU.1 Timing of authentication
- FIA_UID.1 Timing of identification
- FIA_USB.1 User-subject binding
- FIA_AFL.1 Authentication failure handling
- FTP_TRP.1 Trusted path
- FCS_CKM.1 Cryptographic key generation
- FCS_CKM.4 Cryptographic key
- FCS_COP.1 Cryptographic operation

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Extended requirements:

- AccessDatabaseTools Access to the Database Tools
- ControlDatabaseTools Control and supervision of the Database Tools
- FPT_TST_CIMC.2 Software/firmware integrity test
- FPT_TST_CIMC.3 Software/firmware load test

For further details on the security environment definition or on the security requirements, please refer to the Security Target of the TOE.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Architectural Information

As before mentioned, this system has the following described components.

KeyOne CA. Certification Authority

KeyOne CA is an application that provides the Certificate Generation Service, the Revocation Management Service and the Key Recovery Service. Therefore, it allows a CSP, to perform the following tasks:

- To create certificates based on the identity and other attributes of a Subscriber, once verified by the Registration Service. To process requests and reports related to revocation to determine the necessary action to be taken. The results of this service are distributed through the Revocation Status Service.
- To securely store Subscriber keys generated by this KeyOne CA. The stored keys can be recovery through the Key Recovery Service.

The certificates and the CRLs, which are issued by KeyOne CA, are created according to the X.509 v3 certificate format and the X.509 v2 CRL format respectively.

KeyOne LRA: Registration Authority

KeyOne LRA is an application that provides both the Registration Service and the Subscriber Device Provision Service. Therefore, the main goal of this system is to send certification, revocation, suspension and unsuspension requests to KeyOne CA.
For a certification request, the requested certificate can be obtained immediately (online) from KeyOne CA. Once received, KeyOne LRA offers the possibility to store the certificate in a smart card (SSCD).

KeyOne VA. Validation Authority

Key One VA is the application that provides the Revocation Status Service. Therefore, it allows a CSP to provide certificate revocation status information to Relying Parties.
Communication with KeyOne VA takes place according to the OCSP protocol and HTTPS is used as the mechanism for conveying the OCSP messages.

KeyOne TSA SERVER. Time Stamping Authority

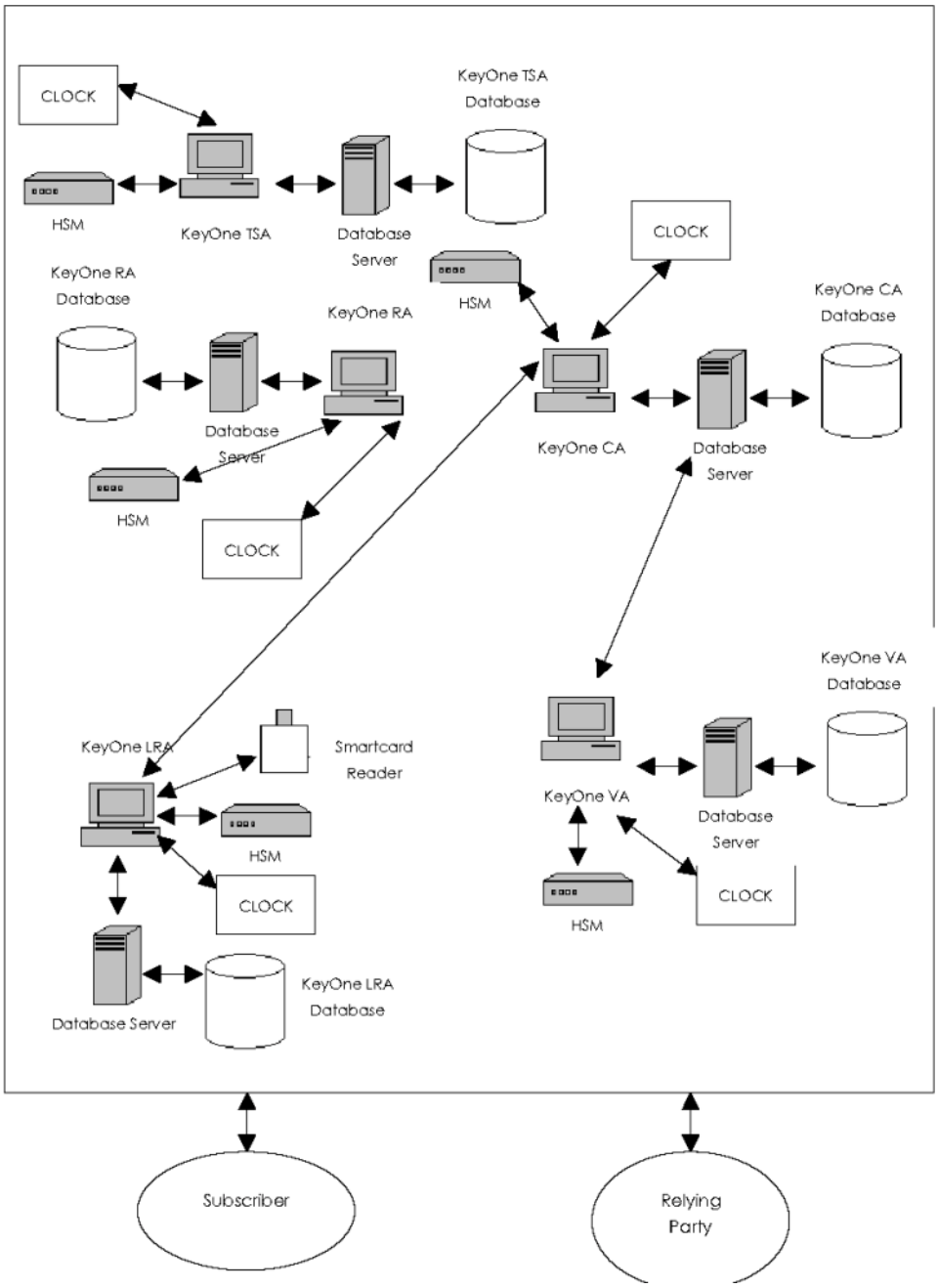
Key One TSA is an application that provides the Time Stamping Service. Therefore, it allows a CSP to create an evidence that a Subscriber's data item existed before a certain point in time (proof of existence).

Communication with KeyOne TSA takes place according to the Time Stamping Protocol and both HTTPS and HTTP are supported as mechanisms for conveying the TSP messages.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Physical Architecture

The physical architecture of the KTS is shown in the figure below.



All KeyOne components are connected to a Database where the information related to the service that the component provides is stored.

The database related to the KeyOne CA component stores generated certificates and CRLs, KeyOne batches (batches contain sets of certification or revocation requests, or certificates, depending on the entity that issued it.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

The main purpose of batches used in KeyOne is to send certification or revocation requests and to receive responses between the RA and the CA and logs generated by the KeyOne CA subsystem.

The database related to the KeyOne VA component stores the status related to the certificates, the messages interchanged with the KeyOne CertStatus component (part of the KeyOne CA product), and the logs generated by the KeyOne VA subsystem.

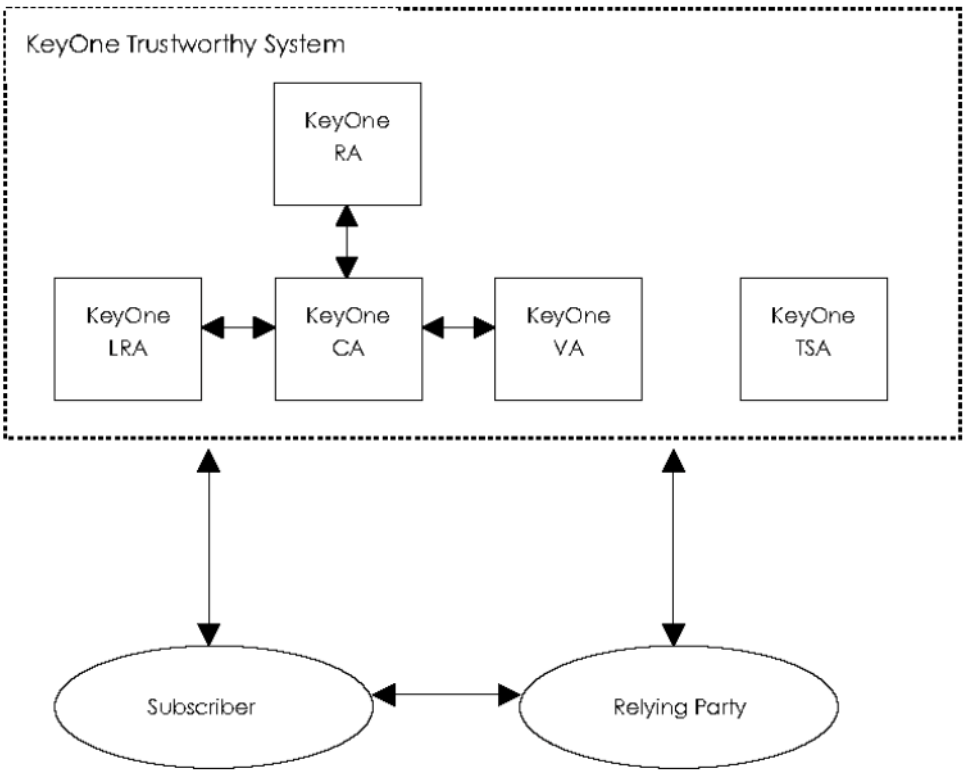
The database related to the KeyOne TSA component stores TSTs requests and responses, and the logs generated by the KeyOne TSA subsystem.
The database related to the KeyOne RA component stores certificates, KeyOne batches and logs generated by the KeyOne RA subsystem.

The database related to the KeyOne LRA component stores logs generated by the KeyOne LRA subsystem.

All KeyOne components are connected to an HSM (Hardware Security Module) in order to generate and store the keys related to the service, and also they are connected to a clock that provides reliable time stamps for the service use.

Logical Architecture

The logical architecture of the KTS is shown in the figure below.



Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Documentation

The product as evaluated is to be shipped with the following documentation, required for the secure installation and operation of the TOE:

- KeyOne 3.0 Installation and Uninstallation Tool Manual, A98558AB 1.18
- KeyOne 3.0 Installation and Administration Manual, 65128EAB 1.6
- KeyOne 3.0 Signing scripts C3133BBD 1.4
- KeyOne 3.0 Batch Format Description, 269C9E2F 1.4
- KeyOne 3.0 CA Administration Manual, 40B3123A 1.23
- KeyOne 3.0 CA User Manual, 8B4B9CFE 1.31
- KeyOne 3.0 Certificate, Keys and CRL Management, EA99A2FE 1.14
- KeyOne 3.0 Console 3999D586 1.23
- KeyOne 3.0 I3D Database Management, DD01D2DA 1.3
- KeyOne 3.0 Logs Registration Administration, 1CBF9472 1.6
- KeyOne 3.0 Master Document, C7342558 1.32
- KeyOne 3.0 RA Administration and User Manual 1.8
- KeyOne 3.0 TSA Administration and User Manual, 7246994C 1.17
- KeyOne 3.0 Template Textual Specification Syntax, E204D730 1.4
- KeyOne 3.0 VA Administration and User Manual, F24E6F5E 1.20
- KeyOne 3.0 CRLA Manual EDFD484B 1.22
- KeyOne 3.0 LRA Administration and User Manual 513BE36C 1.19

IT Product Testing

Both, developer and ITSEF carried out tests on the product. This tests are divided into two categories: functional tests and penetration tests.

Functional Tests

ITSEF verified that functional tests, documented and carried out by the developer was suficient to demonstrate that TOE was sistematically tested according its functional specification. In addition, ITSEF verified the results obtained by the developer.

Penetration Tests

ITSEF carried out several penetration tests against TOE, searching for vulnerabilities o trying exploit the vulnerabilities assessed by developer analisys.
As conclusions of those tests ITSEF stated that vulnerabilities are not exploitable according to the intended usage environment.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Evaluated Configuration

The TOE evaluated configuration is based on the elements described below:

Subsystem	OS	Database	HSM	SCD/SSCD
KeyOne CA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4
KeyOne LRA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4
KeyOne RA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4
KeyOne VA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4
KeyOne TSA	Microsoft Windows 2000	Oracle 9i	nCipher nShield F3 Ultrasign SCSI, firmware version 2.0.5, Hardware version nC4032W	STARCOS SPK 2.4

Additionally, it is necessary the following components:

- NTP client installed in the same host where the KeyOne CA, KeyOne RA, KeyOne LRA, KeyOne TSA and KeyOne VA subsystems.

- Reliable clock that obtains the Co-ordinated Universal Time from a reliable source, and that synchronizes the system clock by means the NTP protocol, using the NTP client installed in the same machine that the KeyOne CA, KeyOne RA, KeyOne LRA, KeyOne TSA and KeyOne VA subsystems.

- Windows 2000 Service Pack 4 for the KeyOne CA, KeyOne LRA, KeyOne RA, KeyOne VA and KeyOne TSA components.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Results of the Evaluation

All the assurance components required by the level EAL4+ (augmented with ALC_FLR.2) present the “PASS” verdict. Consequently, the laboratory (CESTI /INTA) assigns the “PASS” verdict to the whole evaluation with all the evaluator actions being satisfied for the EAL4 methodology, as defined by the third part of the Common Criteria and the Common Evaluation Methodology.

Compliance with the **[**CIMC], Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003, has also been evauated, and assigned a “PASS” verdict.

Evaluator Comments/Recommendations

Conclusions

According to the evaluation carried out by CESTI, it is concluded that, at this moment:

- All activities has a “PASS” verdict . So the evaluator team has assigned a PASS verdict to the evaluation of KeyOne 3.0 04S2R1 with patches B01, B02, B03, B04, B05, B06 and B07 product.

- The TOE KeyOne 3.0 04S2R1 with patches B01, B02, B03, B04, B05, B06 and B07 satisfies its Security Target, SECURITY TARGET KeyOne 3.0 (B4E6DBC0), 1.38, according to CC, EAL4+ (ALC_FLR.2), SOF Basic.

- The TOE KeyOne 3.0 04S2R1 with patches B01, B02, B03, B04, B05, B06 and B07 conforms to the requirements for the protection profile CIMC.

- The result of the evaluation, collected in this ETR, are valid only for the evaluated product as follows:

    - Product: KeyOne 3.0 04S2R1 with patches B01, B02, B03, B04, B05, B06 and B07.
    - Security Target: SECURITY TARGET KeyOne 3.0 (B4E6DBC0), 1.38.

Recommendations

In order to fulfill with the EAL4+ security guarantees of the KeyOne product included in SECURITY TARGET KeyOne 3.0 (B4E6DBC0), 1.38, the license file used in the TOE does not have to allow the execution of scripts launched in unsecure mode (activation of the –unsecure flag).

For secure usage of the TOE, the fulfillment of the assumptions about the environment in the Security Target has to be taken into account. These requirements are stated in SECURITY TARGET KeyOne 3.0 (B4E6DBC0), 1.38 section 3 ’TOE

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Security Environment' (this section incorporate all assumptions about the environment that appears in CIMC, Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.)

For secure usage of the TOE, the fulfillment of the security objectives for the environment in the Security Target has to be taken into account. These requirements are stated in SECURITY TARGET KeyOne 3.0 (B4E6DBC0), 1.38 section 4.2 'Security Objectives for the Environment' and section 4.3 'Security Objectives for both the TOE and the Environment' (this section incorporate all security objectives for the environment that appears in CIMC, Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.)

For secure usage of the TOE, the fulfillment of the security requirements for the IT environment has to be taken into account. These requirements are stated in SECURITY TARGET KeyOne 3.0 (B4E6DBC0), 1.38 section 5.2 'Security Requirements for the Environment' (this section incorporate all security requirements for the IT environment that appears in CIMC, Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003.) For secure usage of the TOE it is very important that persons who are responsible of IT environment elements (basically, operative system, database and HSM) know how each of this elements must be configured in order to give the necessary support to the TOE.

In this product there is not a clear Administrator and a clear User; there are users with a role that have the privileges that their role allows them and therefore they can carry out or not an action depends of the privileges that this action demands. So, in general, there are no independent Administrator Manual and User Manual and in the common document Administrator and User Manual there are no clear and independent sections for each one. This manual is a description of the functionality for the application and, for each step, it is said if a specific role is needed for carrying it out.

For a good understanding of users guides and developer testing documentation, it is very important to make clear that KeyOne 3.0 04S2R1 with patches B01, B02, B03, B04, B05, B06 and B07 is a product developed to work with several security policies defined by the developer. At least, it is possible to work with two different security policies: [CWA] and [CIMC], each one with its own profile. In the context of this evaluation, only [CIMC] policy applies, but in relation with roles there is no a well-defined use of its names and, so, sometimes role names from both policies are used.

In order to make it clear, it is important to say that, where in [CIMC] policy there are four roles: Administrator, Officer, Auditor and Operator,

- Administrator role would be the System Administrator and Security Officer.
- Officer role would be Registration Officer.
- Auditor would be System Auditor.
- Operator role would be System Operator.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

The FPT_CIMC_TSP.1.3 security requirement is accomplished because for each modification (addition, update or delete) of a database registry, the i3D mechanism assures the generation of a digital signature that guarantees the database integrity, then KeyOne system works as if it was configured at the maximum frequency, and therefore the frequency most secure (refinement of the FPT_CIMC_TSP.1.3 requirement).

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

Certifier Recommendations

At the light of the results of the evaluation, and after checking that the security properties of the product, as well as the developer evidence and the applied development practices fulfill with the requirements stated in the Security Target, including the compliance of the **[**CIMC], Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+, october 2003, a positive resolution is proposed for the certification request of the KeyOne 3.0 product as identified in section 2.

Glossary

CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CESTI	Centro de Evaluación de la Seguridad de las Tecnologías de la Información
CIMC	Certificate Issuing and Management Components
CPS	Certification Practices Statement
DPC	Declaración de Prácticas de Certificación
DS	Declaración de Seguridad
ETR	Evaluation Thecnical Report
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
KTS	KeyOne Trusted System
INTA	Instituto Nacional de Técnica Aeroespacial
LRA	Local Registry Authority
NIST	National Institute of Standards and Technology
NPKI	NATO PKI
NTP	Network Time Protocol
OC	Organismo de Certificación
OCSP	On-line Certificate Status Protocol
OE	Objeto de Evaluación
PC	Política de Certificación
PKI	Public Key Infrastructure
PP	Perfil de Protección
RA	Registry Authority
TI	Tecnologías de la Información
TOE	Target Of Evaluation
TSA	Time Stamping Authority
UTC	Universal Time Coordinated
VA	Validation Authority

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es

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 2.2, rev 256, January 2004.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.2, rev 256, January 2004.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.2, rev 256, January 2004.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 2.2, rev 256, January 2004.

[CIMC] Certificate Issuing and Management Components Family of Protection Profiles v1.0, Level 3, EAL 3+.

Security Target

It is published jointly with this certification report the “Security Target of KeyOne 3.0”, code B4E6DBC0, version 1.38.

Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: organismo.certificacion@cni.es