REF: 2009-3-INF-512 V1
Distribution: Public
Date: 24.08.2010

Created: CERT8
Reviewed: TECNICO
Approved: JEFEAREA

# CERTIFICATION REPORT FOR TRUSTEDX v3.0.10S1R1_T (virtual and HW appliance versions)

Dossier: 2009-3 TrustedX

References:

| | |
|---|---|
| EXT-715 | Certification Request |
| EXT-1039 | Evaluation Technical Report |
| CCRA | Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000. |

Certification report of TRUSTEDX v3.0.10S1R1_T (virtual and HW appliance versions), as requested by SAFELAYER SECURE COMMUNICATIONS, S.A. in [EXT-715] dated 06/03/2009, and evaluated by the laboratory Epoche & Espri, as detailed in the Evaluation Technical Report [EXT-1039] received on July 27th 2010, and in compliance with [CCRA].



ENAC CERTIFICACIÓN Nº 45/C-PR110

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

## Table Of Contents





ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

# Summary

This document constitutes the Certification Report for product TRUSTEDX v3.0.10S1R1_T (virtual and HW appliance versions) developed by SAFELAYER SECURE COMMUNICATIONS, S.A.

**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

**Protection Profile**:

U.S. Government Basic Robustness PKE with the packages listed below at Basic Robustness Assurance, EAL4 with ALC_FLR.2 augmentation, Mayo 2007, version 2.8.

- CPV-Basic
- CPV – Basic Policy
- PKI Signature generation
- PKI Signature verification
- PKI Encryption using Key Transfer Algorithms
- PKI Decryption using Key Transfer Algorithms
- PKI Based Entity Authentication
- OCSP Client
- CRL Validation
- Audit
- Continuous Authentication

**Evaluation Level**: EAL4+ (ALC_FLR.2).

Evaluation end date: 23/07/2010.

All the assurance components required by the level EAL4+ (augmented with ALC_FLR.2) have been assigned a “PASS” verdict. Consequently, the laboratory (Epoche & Espri) 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].



ENAC CERTIFICACIÓN Nº 45/C-PR110

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

Considering the obtained evidences during the instruction of the certification request of the TRUSTEDX v3.0.10S1R1_T (virtual and HW appliance versions) product, a positive resolution is proposed.



ENAC
CERTIFICACIÓN
Nº 45/C-PR110

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

## *TOE Summary*

TrustedX includes a comprehensive set of trusted services based on Public Key Infrastructures (PKI) that are standard and service-oriented for any type of consumer, whether an end-user, application or another service:

- Authentication and authorization. Exchanging authentication and authorization information between corporate applications and external security domains, enabling web single sign-on (SSO) using the standards defined by OASIS.
- Key management. Provides the functions to manage the keystores of the TrustedX entities, such as users and applications (key generation, certificate request, certificate import and key import).
- Digital certificate validation. Recognition of multiple certification service providers, providing the information associated with the certificates in a uniform manner. Supports the standard certificate validation mechanisms and accepts the integration of any other personalised mechanism.
- Electronic signature. Supports most of digital signature formats for documents, email and web messaging; including multiple signatures, time-stamped signatures and advanced electronic signatures.
- Electronic signature custody. Custody service for the electronic signatures of documents that maintains their validity for long periods of time using advanced signatures, thus implementing long-term electronic signatures to be able to validate the signature once the digital certificates have expired.
- Data encryption. Information protection using encryption mechanisms, whether for electronic documents, e-mail or web messaging.
- Auditing and accounting. Service that manages log information generated by every platform service component, as well as information regarding their use and/or consumption in a centralised, uniform, secure manner.
- Object and entity management. Broker offering a uniform XML view of objects and entities managed by the platform, completely masking data-specific formats (XML, ASN.1, Text, etc.) and information sources (LDAP, SQL, Files, etc.) and allowing them to be used as web services.

## *Security Assurance Requirements*

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

| Assurance Class | Assurance Components |
|---|---|
| Security Target | ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.2, |



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

| | |
|---|---|
| | ASE_ECD.1, ASE_REQ.2 and ASE_TSS.1 |
| Development | ADV_ARC.1, ADV_FSP.4, ADV_IMP.1 and ADV_TDS.3 |
| Guidance | AGD_OPE.1 and AGD_PRE.1 |
| Life Cycle | ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1 and ALC_FLR.2 |
| Tests | ATE_COV.2, ATE_DPT.1, ATE_FUN.1 and ATE_IND.2 |
| Vulnerability Analysis | AVA_VAN.3 |

## *Security Functional Requirements*

The product security functionality satisfies several requirements as stated by its Security Target, and according to CC Part 2 [CC-P2]:

| | |
|---|---|
| FDP_CPD_(EXT).1 | Certification path development |
| FDP_DAU_CPI_(EXT).1 | Certification path initialization - basic |
| FDP_DAU_CPV_(EXT).1 | Certificate processing – basic |
| FDP_DAU_CPV_(EXT).2 | Intermediate certificate processing – basic |
| FDP_DAU_CPO_(EXT).1 | Certification path output – basic |
| FDP_DAU_CPI_(EXT).2 | Certification path initialisation – basic policy |
| FDP_DAU_CPO_(EXT).2 | Certification path output – basic policy |
| FDP_ETC_SIG_(EXT).1 | Export of PKI Signature |
| FDP_ITC_SIG_(EXT).1 | Import of PKI Signature |
| FDP_DAU_SIG_(EXT).1 | Signature Blob Verification |
| FDP_ETC_ENC_(EXT).1 | Export of PKI Encryption – Key Transfer Algorithms |
| FDP_DAU_ENC_(EXT).1 | PKI Encryption Verification – Key Transfer |
| FDP_ITC_ENC_(EXT).1 | Import of PKI Encryption – Key Transfer Algorithms |
| FIA_UAU.1 | Timing of authentication |
| FIA_UAU.4 | Single-use authentication mechanisms |
| FIA_UAU_SIG_(EXT).1 | Entity Authentication |
| FIA_UID.1 | Timing of identification |
| FDP_DAU_OCS_(EXT).1 | Basic OCSP Client |
| FDP_DAU_CRL_(EXT).1 | Basic CRL Checking |
| FAU_GEN.1-NIAP-0407:2 | Audit data generation – TOE |
| FAU_GEN.2-NIAP-0410:2 | User identity association – TOE |
| FIA_UAU.6 | Re-authenticating |
| FDP_ACC.1 | Subset access control |
| FDP_ACF.1 | Security attribute based access control |



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

| | |
|---|---|
| FTP_TRP.1 | Trusted path |
| FMT_MSA.1 | Management of security attributes |
| FMT_MSA.3 | Static attribute initialization |
| FMT_SMR.1 | Security management roles |
| FMT_SMF.1 | Specification of Management Functions |
| FPT_TEE.1 | Testing of external entities |



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

# Identification

**Product**: TRUSTEDX v3.0.10S1R1_T (virtual and HW appliance versions).

**Security Target:** Security Target – TrustedX, 0775BA94 v1.7, 15-07-2010.

**Protection Profile**:

U.S. Goverment Basic Robustness PKE with the packages listed below at Basic Robustness Assurance, EAL4 with ALC_FLR.2 augmentation, Mayo 2007, version 2.8.

- CPV-Basic
- CPV – Basic Policy
- PKI Signature generation
- PKI Signature verification
- PKI Encryption using Key Transfer Algorithms
- PKI Decryption using Key Transfer Algorithms
- PKI Based Entity Authentication
- OCSP Client
- CRL Validation
- Audit
- Continuous Authentication

**Evaluation Level**: CC v3.1 r2 EAL4+ (ALC_FLR.2).

# Security Policies

The usage of TRUSTEDX v3.0.10S1R1_T product implies to implement a series of organizational policies that assure the commitment of different demands of security.

The details about them are included in the Security Target. In synthesis, the necessity settles down to implement organizational policies relative to:

### Policy 01: P.ACCESS_BANNER

The IT Environment shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

### Policy 02: P.ACCOUNTABILITY

The authorized users of the TOE shall be held accountable for their actions within the TOE.

### Policy 03: P.CRYPTOGRAPHY

Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

## 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, and briefly described below. These same 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.

### Assumption 01: A.Configuration

The TOE will be properly installed and configured.

### Assumption 02: A.Enhanced-Basic

The attack potential on the TOE is assumed to be ”Enhanced-Basic”.

### Assumption 03: A.NO_EVIL

Administrators are non-hostile, appropriately trained and follow all administrator guidance.

### Assumption 04: A.PHYSICAL



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

It is assumed that the environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

## *Threats*

The following threats are not an exploitable risk for the product although the attacks are done by agents with a attack potential of Enhanced-Basic of EAL4, and always under the assumptions and organizational policies listed.

For any threat not included in this list the result of the evaluation nor the corresponding certificate guarantee any resistance.

Threats covered:

### Threat 01: T.AUDIT_COMPROMISE

A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.

### Threat 02: T.CHANGE_TIME

An unauthorized user may change the TSF notion of time resulting in accepting old revocation information or expired certificates.

### Threat 03: T.CRYPTO_COMPROMISE

A user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.

### Threat 04: T.MASQUERADE

A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.

### Threat 05: T.POOR_TEST

Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

### Threat 06: T.RESIDUAL_DATA

A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.

### Threat 07: T.TSF_COMPROMISE

A user or process may cause, through an unsophisticated attack, TSF data, security attributes, or executable code to be inappropriately accessed (viewed, modified, or deleted).

### Threat 08: T.UNATTENDED_SESSION

A user may gain unauthorized access to an unattended session.

### Threat 09: T.UNAUTHORIZED_ACCESS

A user may gain access to user data for which they are not authorized according to the TOE security policy.

### Threat 10: T.UNIDENTIFIED_ACTIONS

The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.

### Threat 11: T.Certificate_Modi

An untrusted user may modify a certificate resulting in using a wrong public key.

### Threat 12: T.DOS_CPV_Basic

The revocation information or access to revocation information could be made unavailable, resulting in loss of system availability.

### Threat 13: T.Expired_Certificate

An expired (and possibly revoked) certificate as of TOI could be used for signature verification.

### Threat 14: T.Untrusted_CA



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

An untrusted entity (Certification Authority (CA)) may issue certificates to bogus entities, permitting those entities to assume identity of other legitimate users.

### Threat 015: T.No_Crypto

The user public key and related information may not be available to carry out the cryptographic function.

### Threat 016: T.Path_Not_Found

A valid certification path is not found due to lack of system functionality.

### Threat 17: T.Revoked_Certificate

A revoked certificate could be used as valid, resulting in security compromise.

### Threat 18: T.User_CA

A user could act as a CA, issuing unauthorized certificates.

### Threat 19: T.Unknown_Policies

The user may not know the policies under which a certificate was issued.

### Threat 20: T.Clueless_PKI_Sig

The user may try only inappropriate certificates for signature verification because the signature does not include a hint.

### Threat 21: T.Assumed_Identity_PKI_Ver

A user may assume the identity of another user in order to verify a PKI signature.

### Threat 22: T.Clueless_PKI_Ver

The user may try only inappropriate certificates for signature verification because hints in the signature are ignored.

### Threat 23: T.Assumed_Identity_WO_En

A user may assume the identity of another user in order to perform encryption using Key Transfer algorithms.

### Threat 24: T.Clueless_WO_En



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

The user may try only inappropriate certificates for encryption using Key Transfer algorithms in absence of hint.

### Threat 25: T.Garble_WO_De

The user may not apply the correct key transfer algorithm or private key, resulting in garbled data.

### Threat 26: T.Assumed_Identity_Auth

A user may assume the identity of another user to perform entity based authentication.

### Threat 27: T.Replay_Entity

An unauthorized user may replay valid entity authentication data.

### Threat 28: T.DOS_OCSP

The OCSP response or access to the OCSP response could be made unavailable, resulting in loss of system availability.

### Threat 29: T.Replay_OCSP_Info

The user may accept an OCSP response from well before TOI resulting in accepting a revoked certificate.

### Threat 30: T.Wrong_OCSP_Info

The user may accept a revoked certificate or reject a valid certificate due to a wrong OCSP response.

### Threat 31: T.DOS_CRL

The CRL or access to CRL could be made unavailable, resulting in loss of system availability.

### Threat 32: T.Replay_Revoc_Info_CRL

The user may accept a CRL issued well before TOI resulting in accepting a revoked certificate.

### Threat 33: T.Wrong_Revoc_Info_CRL



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

The user may accept a revoked certificate or reject a valid certificate due to a wrong CRL.

### Threat 34: T.PKE_Accountability

The PKE related audit events cannot be linked to individual actions.

### Threat 35: T.Hijack

An unauthorized user may hijack an authenticated session.

### Threat 36: T.DISCLOSURE_ OR_NOT_UNIQUE_PRIVATE_KEYS

A private key is improperly disclosed or it can be obtained again (it is not assured that the signature-creation data used for signature generation can practically occur only once).

### Threat 37: T.ILEGITIMATE_USE_OF_PRIVATE_KEYS

An attacker can access to the private keys of users, so that the signatures can be generated without the legitimate signatory consent.

### Threat 38: T.DATA_TO_BE_SIGNED

An attacker modifies the data to be signed while in the process of being signed.

### Threat 39: T.DATA_USED_FOR_VERIFYING_THE_SIGNATURE

The data used to verify the signature do not correspond to the data presented to the verifier.

### Threat 40: T.RESULT_OF_THE_SIGNATURE_VALIDATION

The result of the validation of a signature does not correspond to the result presented to the verifier.

### Threat 41: T.SIGNATORY'S_IDENTITY

The signatory's identity does not correspond to the result presented to the verifier.

### Threat 42: T.SECURITY_AUDIT_EVENTS

The security-relevant changes are not detected.



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

### Threat 43: T.INVALID_CERTIFICATE

The authenticity and validity of the certificate required at the time of signature verification are not reliably verified.

### Threat 44: T.SIGNATURE_NOT_RELIABLY_VERIFIED

The signatures are not reliably verified.

### Threat 45: T.SIGNATURE_FALSIFIED

The signatures can be falsified and the private keys can be derived using currently available technology.

### Threat 46: T.SIGNED_DATA_FALSIFIED

The signed data established by the verifier can be falsified.

### Threat 47: T.PSEUDONYM_NOT_SUPPORTED

It is not assured, at the time of the signature verification, that a pseudonym could be indicated.

## *Operational environment objectives*

The product requires the cooperation from its operational environment to fulfil the requirements listed in its Security Target. This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. These security objectives are assumed by the Security Target to be permanently in place in the TOE environment.

With this purpose, the security objectives declared for the TOE environment are the following:

### Objective 01: P.ACCESS_BANNER

The IT Environment shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

### Objective 02: P.ACCOUNTABILITY



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

The authorized users of the TOE shall be held accountable for their actions within the TOE.

### Objective 03: P.CRYPTOGRAPHY

Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

## TOE Architecture

The TOE consists of a set of Web service components that handles all its functionality. The components are as follows (the following sections contain a detailed description of each one):

**TrustedX Authentication & Authorization (TWS-AA)**. Authentication and authorization service that includes authentication mechanisms using login/password and certificate (TLS/SSL), both used in a direct standard manner, as well as additional mechanisms based on signatures with X.509 certificates. TrustedX can be easily extended with other authentication mechanisms, such as OTP (one-time passwords), biometrics, etc. These additional mechanisms are not included in the current TOE.

**TrustedX Entity Profiler (TWS-EP)**. Information management service providing uniform object and/or entity profiles: users, applications, Web services, policies, certificates, logs/audits, etc., which results in a uniform and controlled method for accessing all configuration and audit data.

**TrustedX Digital Signature (TWS-DS)**. Document digital signature service supporting the generation of different recognized “basic” signature formats (PKCS#7/CMS, PDF Signature, CAdES, XML-DSig/XAdES, S/MIME and WS-Security).

**TrustedX Digital Non-Repudiation (TWS-DR)**. Advanced digital signature service adding reliable time and revocation information to previously-signed documents as a basis for long-term digital signatures. It supports the generation of different recognized “advanced” signature formats (AdES-EPES, AdES-T, AdES-C, AdES-XL



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

and AdES-A), where AdES stands for advanced electronic signature and applies to CAdES (CMS AdES) and XAdES (XML AdES) signature formats.

**TrustedX Digital Signature Verification (TWS-DSV)**. Digital signature verification service (including basic and advanced or long-term digital signatures), regardless of the supplier or the certificate and signature format verification mechanisms. It supports all the formats generated by the TWS-DS and TWS-DR components.

**TrustedX Digital Signature Custody (TWS-DSC).** Custody service for the digital signatures of documents that maintains their validity for long periods of time, thus implementing long-term digital signatures.

**TrustedX Digital Encryption (TWS-DE)**. Document encryption and decryption service in PKCS #7/CMS, S/MIME, XML-Enc and WS-Security formats.

**TrustedX Key Management (TWS-KM)**. Provides the functions to securely manage the keystores of the TrustedX entities, such as users and applications (key generation, certificate request, certificate import and key import). These actions can be performed with an on-disk keystore or a keystore based on a HSM device.

The TrustedX platform provides a common management system that includes configuration, monitoring and access control for each service component. The system presents the following features:

- In order to maintain an open and customizable architecture, XML language is used for configuration, customization, monitoring, and audit and control data. This applies to any type of data stored or exchanged at control ports of online services. TWS-EP is the service component devoted to this function.
- Services are accessed through SOAP according to the WSDL specification of each service. Access is controlled using an authentication token that was previously requested from the TWS-AA service. Client–server interaction is performed via HTTP or HTTPS transport, thus enabling the channel to be secured with SSL/TLS with or without mutual authentication. For example, if login/password authentication is requested, it is recommended to use SSL/TLS.

Each TrustedX service component can interact with other corporate or external infrastructure elements, namely:

**Trusted Third Parties (TTP)**, to which the TOE connects to validate the digital certificates (certification authorities (CA) or validation authorities (VA)) and to obtain time-stamps (time-stamp authorities (TSA)).

The TOE can operate with an external **cryptographic device (HSM)**.



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

**Database (SQL and FILE)**, where the TOE stores log data on the activity of the TrustedX platform's service components for auditing. This data is accessed transparently by the TOE using the TWS-EP component and can be mapped to SQL or FILE physical repositories.

**Document Management System (DMS/ECM)**, where the digital signature custody service component can store and manage the documents with signatures, and the encryption component can store encrypted documents. This data is accessed transparently by the TOE using the TWS-EP component and can be mapped to DMS/ECM (or any WebDAV compliant) or SQL physical repositories.

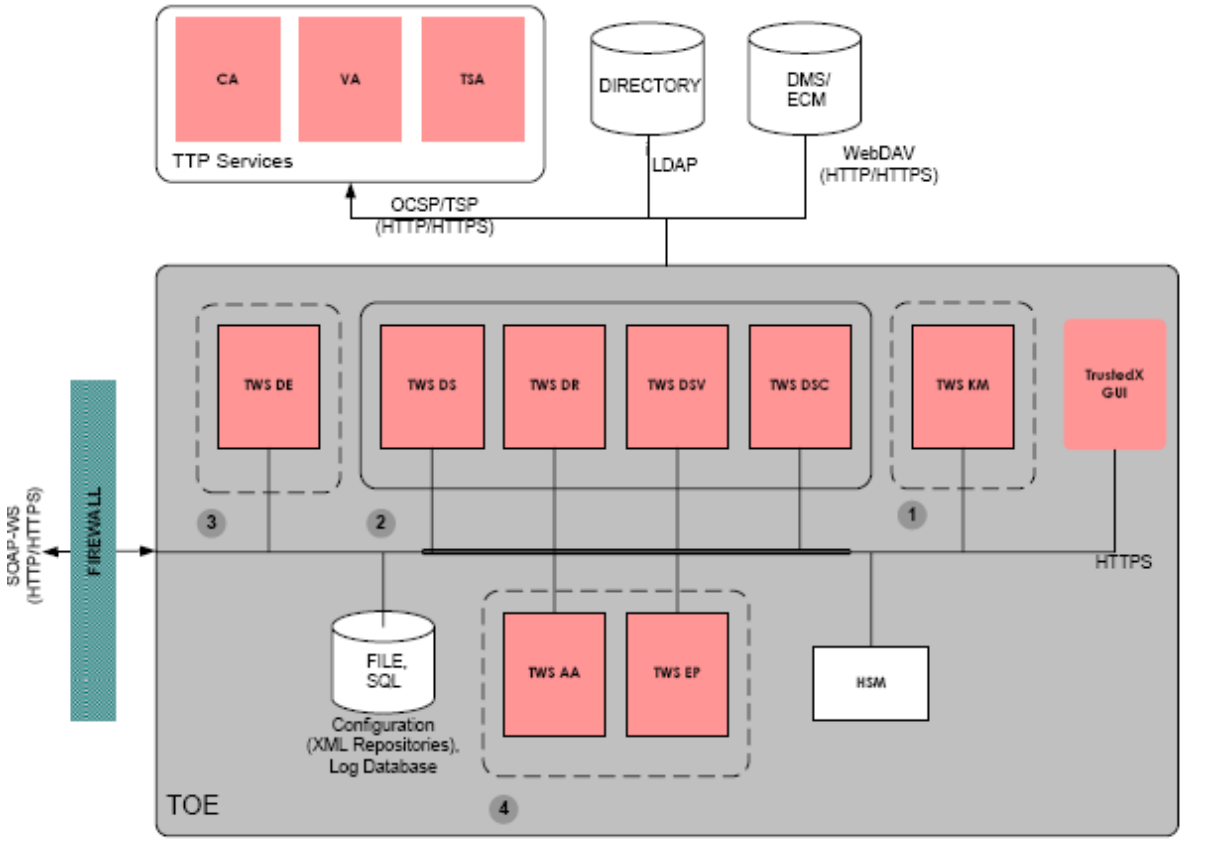
**Directory**, from/to where the TOE can read and write data on the entities (individuals, applications or Web services) recognized by the platform. This information is accessed transparently by the TOE using the TWS-EP component and can be mapped to LDAP, SQL or FILE physical repositories.

The figure below illustrates the interaction between the mentioned infrastructure elements with the TOE. It also shows interactions with the corporate applications that use the TOE's services. There is also the option, especially for greater numbers of applications and/or if different authentication mechanisms are required, to have an authentication/authorization agent to centralize some or all of the authentication and authorization functions required by the applications.



ENAC
CERTIFICACIÓN
Nº 45/C-PR110

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




1. Key Management
2. Digital certificate validation, advanced signature generation and verification and signature custody
3. Encryption and decryption
4. Entity Management, authentication and authorization



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

## Documents

The basic documentation distributed with the TOE to be used with the security assurance provided by the certificate issued is:

TrustedX Appliance Edition - Integración
TrustedX Appliance Edition - Configuración en alta disponibilidad

TrustedX Appliance Edition - Requisitos Técnicos de la release 3.0.10S1R1_T

TrustedX Appliance Edition - Perfiles DSS
TrustedX Appliance Edition - Servicio de gestión de claves

TrustedX Appliance Edition - Casos de uso
TrustedX Appliance Edition - Manual del intérprete de comandos

TrustedX Appliance Edition - Guía de documentación

TrustedX Appliance Edition - Perfiles DE
TrustedX Appliance Edition - Servicio de gestión de claves simétricas

TrustedX Appliance Edition - Administración

TrustedX Appliance Edition - Introducción
TrustedX Appliance Edition - Rendimiento
TrustedX Appliance Edition - Tutorial de SmartWrapper

TrustedX Appliance Edition - Notas de la release 3.0.10S1R1_T

TrustedX Appliance Edition – Tutorial de SmartGateway

TrustedX Appliance Edition - Instalación y puesta en marcha

TrustedX Appliance Edition - Políticas
TrustedX Appliance Edition - Conceptos
TrustedX Appliance Edition - Manual de Referencia

TrustedX Appliance Edition – Servicio de custodia de firmas

TrustedX Appliance Edition - Perfil de firma PDF

TrustedX Appliance Edition – Tutorial de configuración

TrustedX Appliance Edition - Servicio de integración de información

TrustedX Appliance Edition - Manual de integración de XAM



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

## TOE Testing

The manufacturer has developed testing for the TOE TSF. All these tests have been performed by the manufacturer in their location and facilities with success.

The process has 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 is been checked also that the obtained results during the tests fit or correspond to the previously estimated results.

The evaluator examined the design specification and test documentation, concluding that all the modules functionality (low level design) are tested. Therefore, all TSFIs are fully tested. The evaluator verified that TSFI were tested in test plan. The test procedures mapped all TSFI to SFR-enforcing modules.

The evaluator has repeated all the tests defined in the TOE test specification according to the different configurations defined the developer. All tests have been successfully performed.

## TOE Configuration

The environment components selected for the evaluation of this product are the following:

- Operating System: Red Hat Enterprise Linux Version 5.3 with the Tomcat 6.0.26 Web server and the JBoss 5.1.0 application server.
- Databases: Any DBMS supporting a well-defined JDBC interface with SSL/TLS support, for instance, Microsoft SQL Server or Oracle.
- Hardware Security Module: ncipher nShield F3 2000 for netHSM (FIPS 140-2 level 3 hardware cryptographic module).
- Document Management System: Any documental server (DMS/ECM) accessible by means of an access interface based on HTTP/WebDAV defined for TrustedX, for instance, Oracle Content Database.



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

- Directory: Any directory compliant with the RFC 4511 ("Lightweight Directory Access Protocol (LDAP): The Protocol") with SSL/TLS support, for instance, SunOne Directory Server.
- Optionally (only if the services of a time stamping authority are required): any TSA compliant with the TSP protocol (see [RFC3161]).
- For the Hardware Appliance Edition, it is necessary to use computers3 with the following characteristics: A processor with x86-64 compatible architecture, two network interfaces (minimum) and a DVD reader.
- Clients making requests to the TrustedX Web services: Any that correctly validates the certificates for an SSL/TLS connection.

**Software configuration**

The TrustedX security policy is a set of configuration restrictions that must always be met. One of the security policies included in the TOE is the EAL4+ Security Policy. To guarantee the security conditions and the functional requirements included in this Security Target, it is necessary to fix this security policy.

# Evaluation Results

The product TRUSTEDX v3.0.10S1R1_T (virtual and HW appliance versions) has been evaluated in front of the "Security Target – TrustedX, 0775BA94 v1.7", 15-07-2010.

All the assurance components required by the level EAL4+ (augmented with ALC_FLR.2) have been assigned a "PASS" verdict. Consequently, the laboratory (Epoche & Espri) 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].



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

# Comments & Recommendations from the Evaluation Team

Following, some important aspects that might determine the use of the product are described, bearing in mind the scope of the problems found during the evaluation and its security target.

## The concept of the TOE according to its security target.

The TOE security target claims conformance with the protection profile [PP PKE] applicable to PKE (Public Key Enable Applications) products type, whose cryptographic services are provided by a device or external cryptographic module, that shall be FIPS 140-2 validated. The TOE, according to the [PP PKE], is responsible for the invocation of the device to provide the cryptographic services that the users demand. In addition, the module provides security mechanisms protecting the cryptographic keys.

The developer includes in his security target, the SFRs required by the [PP PKE] based on the security problem defined and the TOE objectives specification.

The ST includes new threats, the security objectives of the TOE to mitigate these new threats and the SFRs derived from the requirements specified in ANNEX II and III of the EU Directive on electronic signature. It has been not modified, neither the environment, nor the policies specified in [PP PKE]; the new threats included have been mapped to security objectives of the TOE or security objectives of the environment stated in the protection profile.

The evaluation does not demonstrate in any case conformance with the EU Directive on electronic signature. The evaluation only determines that the TOE meet the requirements specified in the security target with the associated assurance established.

There are cases where the mitigation of the new threats included have been addressed together by the TOE and the environment: those in which the protection of the signature service is required and those where the protection and the guarantee of certain security properties of the associated keys are required (both in creation and signature verification). In these cases, the TOE contributes assuring that it is operative only if there is a FIPS 140-2 cryptographic module in the environment, being this, the one that provides the final guarantees with regard to the protection of the service and the cryptographic material. This situation is specified in the security target (see notes in tables 5.31 and 5.33).

With regard to the protection requirements of the digital signature, once it has been exported from the module, the TOE guarantees its protection in transit establishing a trusted channel with the user. When the signature has been imported to the TOE, its



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

protection is resolved by means of the I&A and control of access mechanism of the TOE and the application of the following assumption stated in the [PP PKE]:

| | |
|---|---|
| A.PHYSICAL | It is assumed that the environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE. |

## Mitigation of exploited vulnerabilities, by means of environment assumptions.

The developer details in the security target the applicability of the following assumption (reliable administrators),

| | |
|---|---|
| A.NO_EVIL | Administrators are non-hostile, appropriately trained and follow all administrator guidance. |

specifying the profiles and administration rights to which the assumption is applicable. This implies that certain vulnerabilities have not been fixed modifying the product (they are still present), but they are considered not to be exploitable in an operational environment applying this assumption.

Therefore, all the vulnerabilities resolved by means of the assumption A.NO_EVIL could be exploitable out of the scope of the operational environment of the TOE. Therefore, it is essential the fulfilment of the environment objectives defined in the security target.

## Installation and operation

The TOE can be installed both on a hard disk and on a virtual machine. The content is not encrypted in any case. Therefore, an attacker with physical access to the TOE might modify the hard disk where the TOE is installed and create a new user with administration rights, compromising all the TOE assets.

When the authentication with certificates applies, it would be appropriate the use of password protected certificates, preventing the use of the certificate by a non authorized user. This certificate protection can be activated during the certificate installation in the PC.



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

## Certifier Recommendations

Considering the obtained evidences during the instruction of the certification request of the TRUSTEDX v3.0.10S1R1_T (virtual and HW appliance versions), a positive resolution is proposed.



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@cni.es

# Glossary

**CB** Certification Body

**CC** Common Criteria

**EAL** Evaluation Assurance Level

**IT** Information Technology

**ST** Security Target

**TOE** Target of Evaluation

**TSF** TOE Security Functionality

**PP** Protection Profile

**SAR** Security Assurance Requirement

**SFR** Security Function Requirement

**VM** Virtual Machine



ENAC CERTIFICACIÓN Nº 45/C-PR110
Avenida del Padre Huidobro s/n
Fax: + 34 91 372 58 08
Email: certificación.ccn@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 3.1, r2, September 2007.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r2, September 2007.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r2, September 2007.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r2, September 2007.

[PP PKE] US Government Family of Protection Profiles. Public Key-Enabled Applications For Basic Robustness Environments. May 1, 2007. Version 2.8

# Security Target

It is published jointly with this certification report the security target:
**Security Target – TrustedX, 0775BA94 v1.7, 15-07-2010**



ENAC CERTIFICACIÓN Nº 45/C-PR110

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