Certification Report

EAL 4+ (ALC_FLR.2) Evaluation of

TÜBİTAK BİLGEM UEKAE

ELEKTRONİK SERTİFİKA YÖNETİM ALTYAPISI (ESYA)- ELECTRONIC CERTIFICATE MANAGEMENT INFRASTRUCTURE v2.0

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Certificate Number:TSE-CCCS-031

TABLE OF CONTENTS

Document Information

Date of Issue	***08.09.2015***
Version of Report	***v1.0***
Author	***Cem ERDİVAN***
Technical Responsible	***Zümrüt MÜFTÜOĞLU***
Approved	***Mariye Umay AKKAYA***
Date Approved	***08.09.2015***
Certification Report Number	***21.0.03/15-001***
Sponsor and Developer	***TÜBİTAK BİLGEM UEKAE***
Evaluation Lab	***TÜBİTAK BİLGEM OKTEM***
TOE Name	***ELECTRONIC CERTIFICATE MANAGEMENT INFRASTRUCTURE v2.0***
Pages	***21***

Document Change Log

Release	*Date*	*Pages Affected*	*Remarks/Change Reference*
V1.0	***08.09.2015***	***All***	***First Released***

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 4, using Common Methodology for IT Products Evaluation, version 3.1, revision 4. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BİLGEM OKTEM, which is a public CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for Electronic Certificate Management Infrastructure v2.0 whose evaluation was completed on 18.08.2015 and whose evaluation technical report was drawn up by TÜBİTAK BİLGEM OKTEM (as CCTL), and with the Security Target document with version no 1.6 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on:

http://www.commoncriteriaportal.org

1 - EXECUTIVE SUMMARY

This report constitutes the certification results by the certification body on the evaluation results applied with requirements of the Common Criteria for Information Security Evaluation.

Evaluated IT product name: Electronic Certificate Management Infrastructure
IT Product version: v2.0
Developer's Name: TÜBİTAK BİLGEM UEKAE
Name of CCTL: TÜBİTAK BİLGEM OKTEM
Assurance Package: EAL4+ (ALC_FLR.2)
Completion date of evaluation: 18.08.2015

1.1 Brief Description

ESYA v2.0 (TOE) is an X.509 certificate generation and management system software. TOE provides the following features:

- The important TOE events are logged for further security audit in order to identify the security violations;
- TOE and user public, private and secret keys are protected against unauthorized modification and disclosure using the cryptographic functions provided by the environment;
    - TOE does not store end user public keys, but certificates are digitally signed to protect the exported public keys against unauthorized modifications;
    - Only end user encryption certificates private keys are stored on demand. These keys are stored in the database in a FIPS approved encrypted form which is performed by the hardware cryptographic module;
    - TOE secret keys are stored in the database in an encrypted form which is performed by the soft cryptographic module;
- User data is protected by means of certificate issuance, revocation, recovery;
- Certificate and Certificate Revocation List profiles are managed;
- Persons can not perform TOE Security Functions unless they are properly identified and authenticated;
- Security functions are managed by providing distinct roles in order to maintain the security of TOE;
- The integrity of confidential data are protected from disclosure and modification by means of encryption, reliable time stamps and audit logs;
    - Protection against unauthorized disclosure and modification is provided with encryption and digital signatures;
    - The TOE relies on the system clock of the host for a reliable time stamp. A date/time stamp is included and associated with each audit entry;
    - TOE stores all audit entries in database. Each entry contains log number, event accomplishment status, log date, log description, application name, log signature date, accountable person and log signature information. A keyed message authentication code is created on the appended values of the entry, so that the integrity of the entry is provided. In addition, the exact number of rows in the signed tables is maintained in another table.
- The data transmitted between the TOE and remote users are protected against modification and disclosure.

1. Certification Authority Services
Certification Authority Services:

- Generate X.509 certificates, certificate revocation lists (CRLs),
- Distribute the up-to-date certificates and CRLS.

1.1 Certification Service
Certification Service is a network service which listens a specified port and generates X.509 certificates for valid requests.

1.2 CRL Service
CRL Service revokes the certificates for several reasons and issues CRLS.

1.3 Archive Service
Archive Service archives data for long term usage. Archived data is protected against unauthorized modification.

1.4 CMP
Certificate Management Protocol (CMP) provides on-line interactions between the CA Services and Administration Center/Registration Authority. This infrastructure component is implemented according to RFC 4210 (Internet X.509 Public Key Infrastructure Certificate Management Protocol).

2. Administration Center
Administration center is a GUI application which can be used by the administrators to administrate the Certification Authority. Administration center mainly provides the following functionality:

- Definition, activation, deactivation of administrators, registrars, auditors and their privilege management.
- Configuration of Certification Authority Services
- Definition of Certificate, CRL profiles
- Audit of events to be audited by auditors

3. Registration Authority
Registration Authority can be used by the registrars and end users. It provides the following functionality:

- Application can be started by Administrators.
- Receiving end user and device information and validation for further usage in generating certificate.
- Access through a web based interface for registrars
- Management of end user, device information
- Requesting certificate from the certification server for end user/device
- A web based interface for self requesting certificate for the end users
- Request for revoking or placing a certificate on hold.

4. OCSP(Online Certificate Status Protocol) Server
OCSP Server generates BasicOCSP responses compliant to RFC 2560 in order to give the online certificate status. OCSP Server uses the database as the certificate status source, so that the freshest certificate status can be queried.

1.2 TOE Security Functions

1-Security Audit

1.1-Audit Data Generation

TOE provides the capability to define new or exclude audit events through Administration Center, but definition of new audit events, requires software changes in the TOE. The TOE records all the auditable events to the database whenever it starts up until shut down. Log number, event accomplishment status, log date, log description, application name, log signature date, accountable person and log signature information are stored in the database.

1.2-Accountability of Users

Each audit event is uniquely associated with the identity of the user who caused the event, as appropriate.

1.3-Audit Data Selection

In Administration Center the auditable events can be included or excluded from the set of audited events according to event type.

1.4-Audit Data Protection

TOE stores all audit entries in database. Each entry contains log number, event accomplishment status, log date, log description, application name, log signature date, accountable person and log signature information. A keyed message authentication code is created on the appended values of the entry, so that the integrity of the entry is provided. In addition, the exact number of rows in the signed tables is maintained in another signed table.

Since the integrity of the audit log entry in the audit table, and the integrity of the whole audit table is provided, the audit logs are protected against unauthorized modification and deletion.

The integrity of the audit logs are provided by keyed hash, the hash is generated in every log creation and the hash is also included in the audit log.

1.5-Prevention of Audit Data Loss

Before starting an audited event, the row in the audit database table is reserved so that it is guaranteed that the log for the event can be stored. If the reservation is not possible due to the insufficient disk space or database problem, then the TOE does not execute the event.

1.6-Reliable Time Source

The TOE relies on the system clock of the host for a reliable time stamp. A date/time stamp is included and associated with each audit entry.

2-Roles

2.1-Role Definition

Administrator, Registrar, Auditor are the roles defined in TOE. These roles are defined in detail below:

- **Administrator** administrates Certification Authority Services and Administration Center. They use smartcards which contain signature, encryption key pairs and the corresponding administrator certificates issued by the CA in order to logon the aforementioned applications. Minimum two administrators have to be defined during the setup of TOE: After setup, new administrators can be created, or existing administrators deactivated using the Administration Center with the approval of other administrators. Administrators can also create, deactivate Registrars and Auditors. They are responsible for administration of Certification Authority Services.

- **Registrar** can be defined by the Administrators from the Administration Center. Registrars register and manage the end user information through the Registration Authority application. They create requests to the Certification Authority Services for issuing or revoking certificates.

- **Auditor** can be defined by the Administrators from the Administration Center. Auditors review the audit logs and create reports using the Administration Center application.

Administrators have no privilege restriction while using CA Services and Administration Center. But some of the operations require the approval of more than one administrator. Auditors have the privilege only to check the audit logs and create reports from the Administration Center. Different set of privileges can be assigned to the Registrars from the Administration Center.

2.2-Management of security functions behavior

Administrator, Registrar, Auditor creation, authorization, TOE secret keys management, Certificate, CRL profile management, Audit parameters management can be performed by the security functions.
Certain operations are only available to certain operators.

3-Scope of Policy and Access Rules

Certification Authority Services and Administration Center can be only used by Administrators, and Registration Authority can be only used by Registrars. Auditors can use only the audit related functionality in Administration Center. Registrars can use Registration Authority according to their privileges. The privilege assignments to Registrars are managed in Administration Center.

4-Identification and Authentication

Administrators, Registrars and Auditors need smartcards in order to login to the aforementioned applications. They have signature and encryption key pairs and the corresponding certificates in the smartcards.

Administrators need to enter their id and the smartcard password in the login screen. After successful login to the smartcard, the database password encrypted for the administrators which is stored in the ini file is decrypted with the administrator encryption certificate private key. Administrator id information and the smartcard serial number is checked from the database, so it is assured that the information in the smartcard is not copied. A random number is signed by the administrator, and it is checked against the signature certificate of the administrator in the database. Finally, the role attribute in the signature certificate is checked, and validated against the administrator object identifier.

Registrars need to enter their id and the smartcard password in the login screen. First of all, if the registration authority application is running, Registrars id is checked from the database and if found, smartcard library name, serial number and a random number is sent to the client. With the provided library name, registrar tries to login the smartcard. After login the smartcard serial number is checked, and the random number is signed with the signature certificate. This signature is validated in the registration authority application. Finally, the role attribute in the signature certificate is checked, and validated against the registrar object identifier.

5-Remote Data Entry and Export

TOE generates certificates and the revocation status for them. The security of the transmission of this information to the end users depends on the TLS protocol provided by the IT environment.

During the certificate request and the key recovery, CMP protocol is used which enforces mutual authentication and integrity verification. In TOE, no user has direct access rights to the database. The requests are sent by the Registrars from Registration Authority to CA Services.

5.1-Enforced Proof of Origin and Verification of Origin

The integrity of the information which will be used for generation of a certificate is validated with the table row signature. In the login process of the administrators, registrars and auditors, certificates issued by the CA are used, thus the certificates are validated according to the entries in the trusted database. TOE provides the revocation information by publishing CRLs or giving answers to OCSP request. Integrity, validity and the proof of origin of the certificate status information is provided with the CA signature on the CRLs and OCSP answers.

5.2-Protection of data communications between CA Services and Registration Authority

While TSF transfers security relevant and confidential data between TOE components, CMP is used so that authentication, confidentiality and integrity protection is provided against unauthorized modification and disclosure.

5.3-Trusted channel

The security of the sensitive data transmitted between the TOE and remote entities are provided with the CMP and TLS protocol. To initiate any key management or certificate management transactions a valid authentication code is required. For security-relevant information, the TSF only accepts the information if it was signed using a digital signature algorithm.

6-Certificate Management

6.1-Certificate Generation

TOE only generates certificates whose format complies with X.509 version 3. Proof of possession is always established before a certificate can be made available to an end-user. For X.509 v3 certificates, TOE ensures that:

- SerialNumber is unique,
- notBefore is set to current date and the notAfter value is set current date + validity of the certificate,
- Issuer is set to CA's DN and never contains a null name,
- Subject is set to subject's DN and never contains a null name.

In addition, subjectPublicKeyInfo can be set to contain the OID (object identifier) for FIPS-approved algorithms (RSA/{SHA-1,SHA256,SHA384, SHA512}, ECDSA/{SHA-1,SHA256,SHA384, SHA512}).

Certificates are generated according to certificate profile chosen by the Registrars.

Before generating certificates, TOE verifies that public/private key pairs corresponds to each other.

6.2-Certificate Status Export

TOE exports certificate status information by two ways; CRLs and OCSP responses.

TOE publishes Certificate Revocation Lists (CRLs) in a format that complies with X.509v2.

TOE provides basic OCSP responses in accordance with IETF RFC 2560. The administrator specifies ResponderId in the OCSP server configuration.

6.3-Certificate Profile Management

Using TOEcertificate profiles only certificates which comply with X.509 version 3 can be generated. The certificate profiles are stored in the database, and new profiles can be created by the Administrators.

Administrators are required to specify the key owner's identifier, algorithm identifier for the subject's public/private key pair, the identifier of the certificate issuer, the length of time for which the certificate is valid. They also need to specify keyUsage, basicConstraints and certificatePolicies.

If certificate profile is created accordingly, the user private keys are first encrypted with FIPS 140-2 validated cryptographic module and then stored in the database.

7-Certificate Revocation

7.1-CRL Profile Management

Using TOE CRL profiles, only CRLs which comply with X.509 version 2 can be generated. The CRL profiles are stored in the database, and new profiles can be created by the Administrators. Administrators are required to specify issuer and nextUpdate (lifetime of a CRL) fields to create a CRL profile.

7.2-CRL Validation

CRLs issued by TOE are compliant with X.509 version 2. Issuer is never set to null and set to CA's DN. subjectPublicKeyInfo can be set to contain the OID (object identifier) for FIPS-approved algorithms (RSA/{SHA-1,SHA256,SHA384, SHA512}, ECDSA/{SHA-1,SHA256,SHA384, SHA512}).thisUpdate indicates the issue date of the CRL, nextUpdate is always after thisUpdate.

8-Key Management

8.1-Private Key Protection

Only end user encryption certificates private keys are stored on demand. These keys are stored in the database in a FIPS approved encrypted form. The encryption is performed by the hardware cryptographic module. These keys are exported to end user with CMP protocol.

TOE secret keys are encrypted in FIPS 140-2 level 3 validated hardware cryptographic module and stored in the database in an encrypted form.

TOE triggers cryptographic modules (hardware and software) to perform all cryptographic operations. In the cryptographic modules TOE private and secret key export is not allowed.

8.2-Public Key Protection

TOE does not store end user public keys, but certificates. The user certificates are digitally signed which protects the exported public keys against unauthorized modifications.

8.3-Key Zeroization

TOE does not store plaintext keys. The zeroization of keys are provided by FIPS 140-2 validated Hardware and Software cryptographic modules which are invoked by the TOE.

8.4-Strength of Functions and Cryptographic Operations

TOE uses FIPS validated software cryptographic module for encryption, decryption, hashing, macing, signature verification. These operations are performed in accordance with the following standards

Encryption/decryption: FIPS PUB 197 (AES);
Signature generation/verification: FIPS PUB 186-2 (RSA, ECDSA), Draft FIPS PUB 186-3 (RSA-PSS);
Hashing: FIPS PUB 180-1 (SHA-1), FIPS PUB 180-2 (SHA 224, SHA256, SHA384 and SHA512); and
MACing: FIPS PUB 113

TOE uses FIPS validated hardware cryptographic module for key generation, decryption and signature generation.

1.3 Threats

1-Authorized users

T.Administrative errors of omission addresses errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.

T.User abuses authorization to collect and/or send data addresses the situation where an authorized user abuses granted authorizations by browsing files in order to collect data and/or violates export control policy by sending data to a recipient who is not authorized to receive the data.

T.User error makes data inaccessible addresses a user accidentally deleting user data. Consequently, the user data is inaccessible. Examples include the following:

- User accidentally deletes data by striking the wrong key on the keyboard or by striking the enter key as an automatic response.
- User does not understand the implications of the prompt at hand and inadvertently gives a response that deletes user data.

- User misunderstands a system command and issues a command that unintentionally deletes user data.

T.Administrators, Registrars and Auditors commit errors or hostile actions addresses:

- Errors committed by administrative personnel that directly compromise organizational security objectives, change the technical security policy enforced by the system or application, or
- Malicious obstruction by administrative personnel of organizational security objectives or modification of the system's configuration to allow security violations to occur.

2-System

T.Critical system component fails addresses the failure of one or more system components that results in the loss of system-critical functionality. This threat is relevant when there are components that may fail due to hardware and/or software imperfections and the availability of system functionality is important.

T.Flawed code addresses accidental or deliberate flaws in code made by the developer. Examples of accidental flaws are lack of engineering detail or bad design. An example of a deliberate flaw would be the inclusion of a trapdoor for later entry into the TOE.

T.Malicious code exploitation addresses the threat where 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. The execution of malicious code is done through a triggering event.

T.Message content modification addresses the situation where a hacker modifies information that is intercepted from a communications link between two unsuspecting entities before passing it on to the intended recipient. Several kinds of modification are possible: modification of a single message, deletion or reordering of selected messages, insertion of bogus messages, replay of previous messages, and modification of accompanying message security attributes.

3-Cryptography

T.Disclosure of private and secret keys addresses the unauthorized disclosure of secret and/or private keys.

T.Modification of private/secret keys addresses the unauthorized revision of a secret and/or private key.

T.Sender denies sending information addresses the situation where the sender of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

4-External Attacks

T.Hacker gains access addresses:

- Weak system access control mechanisms or user attributes
- Weak implementation methods of the system access control
- Vulnerabilities found in system or application code that allow a hacker to break into a system undetected.

T.Hacker physical access addresses the threat where an individual exploits physical security weaknesses to gain physical control of system components.

T.Social Engineering addresses the situation where a hacker uses social engineering techniques to gain information about system entry, system use, system design, or system operation.

2 CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

ESYA v2.0(TOE) is an X.509 certificate generation and management system software. TOE and its operational environment provides privacy, access control, integrity, confidentiality, authentication and non repudiation services.

TOE is composed of Certification Authority Services, Administration Center and Registration Authority. TOE is software and it does not include any hardware components.

TOE can be used to provide security in the electronic transactions for the organizations. By implementing asymmetric cryptography and using electronic certificates and cryptographic keys, both TOE and its operational environment enable secure communication between parties. This infrastructure is comprised of certification server and other auxiliary applications. End users are entitled to get a certificate by proving their identities and registering to the TOE. This certificate can be used for electronic signatures and data encryption. TOE and its operational environment provides authentication, non repudiation, message integrity and confidentiality services by means of this infrastructure.

Certificate Number	*21.0.03/TSE-CCCS-31*
TOE Name and Version	*Electronic Certificate Management Infrastructure*
Security Target Document Title	*Elektronik Sertifika Yönetim Altyapisi (ESYA) (Electronic Certificate Management Infrastructure) v2.0 Security Target*
Security Target Version	*1.6*
Security Target Document Date	*13.08.2015*
Assurance Level	*EAL 4+ (ALC_FLR.2)*
Criteria	• *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 4, September 2012* • *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 4, September 2012* • *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 4, September 2012*
Methodology	*Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 4, September 2012*
Protection Profile Conformance	*Certificate Issuing and Management Components (CIMC) Protection Profile, version 1.5, August 11, 2011*
Common Criteria Conformance	• *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012* • *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 4, September 2012, extended.* • *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 4, September 2012, conformant.*

Sponsor and Developer	*TÜBİTAK BİLGEM UEKAE*
Evaluation Facility	*TÜBİTAK BİLGEM OKTEM*
Certification Scheme	*TSE CCCS*

2.2 Security Policy

P.Authorized use of information

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

P.Cryptography and secure storage of cryptographic assets

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

2.3 Assumptions and Clarification of Scope

1-Personnel Assumptions

A.Auditors Review Audit Logs

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

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, Registrars and Auditors

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

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 theTOE and are expected to act in a cooperative manner.

A.CPS

All Administrators, Registrars, and Auditors are familiar with the certificate policy (CP) and certification practices statement (CPS) under which the TOE is operated.

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. TOE assumes that codes signed by any trusted entity is not malicious.

A.Notify Authorities of Security Issues

Administrators, Registrars, 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, registrars and auditors are trained in techniques to thwart social engineering attacks.

2-Connectivity

A.Operating System

The operating system has been selected to provide the functions required by this CIMC to counter the perceived threats identified in this ST.

3-Physical

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.

2.4 Architectural Information

Administration Center Subsystem

AC Subsystem provides an interface which is used by authorized administrators to define TOE settings and by registrars to monitor critical logs. In order to use AC subsystem; certified active administrators who are defined during installation or defined by Administration Center subsystem, must login using their smart cards. Admins decrypt database password which is encrypted for themselves and is located in the ini file, using their smart cards in which signing and encryption certificate are present. On cryptographic operations, FIPS approved NSS v3.12.4 and HSM are used. Admin's information that are received from database, are checked; signature in smart card and admin's signature certificate are also checked. If process is a success, logging in is registered as critical log and system interface is shown.

Registration Authority Subsystem

RA subsystem is where user and device information ,which will receive certificate, are recorded and where certificate requests are made to Services Subsystem. It also transfers certificates to end-users and generates requests to update the certificate status information.

Assistant Subsystem

Assistant Subsystem comprises modules used in TOE and forming the infrastructure.

Online Certificate Status Protocol Subsystem

OCSP Subsystem is an application that queries status information of certificates that are generated by TOE and it runs on a web server. A certificate which is used in an electronic certificate application must be valid. To determine if the certificate is valid or not; the application must access the certificate status information. OCSP is the system that allows clients to query certificate status information online and instantly. An OCSP server can respond to both database or

CRL-based requests. In order to do this first OCSP server requires at least one signature certificate and key because responses have to be signed with a private key. Cryptographic operations within OCSP subsystem are carried out using FIPS-140-2 approved NSS library.

Services Subsystem

Services Subsystem listens requests sent from CMP and generates certificate for the valid ones. Additionally, it periodically checks revocation/suspention/unsuspention requests with CA subsystem and updates concerned certificate's status.

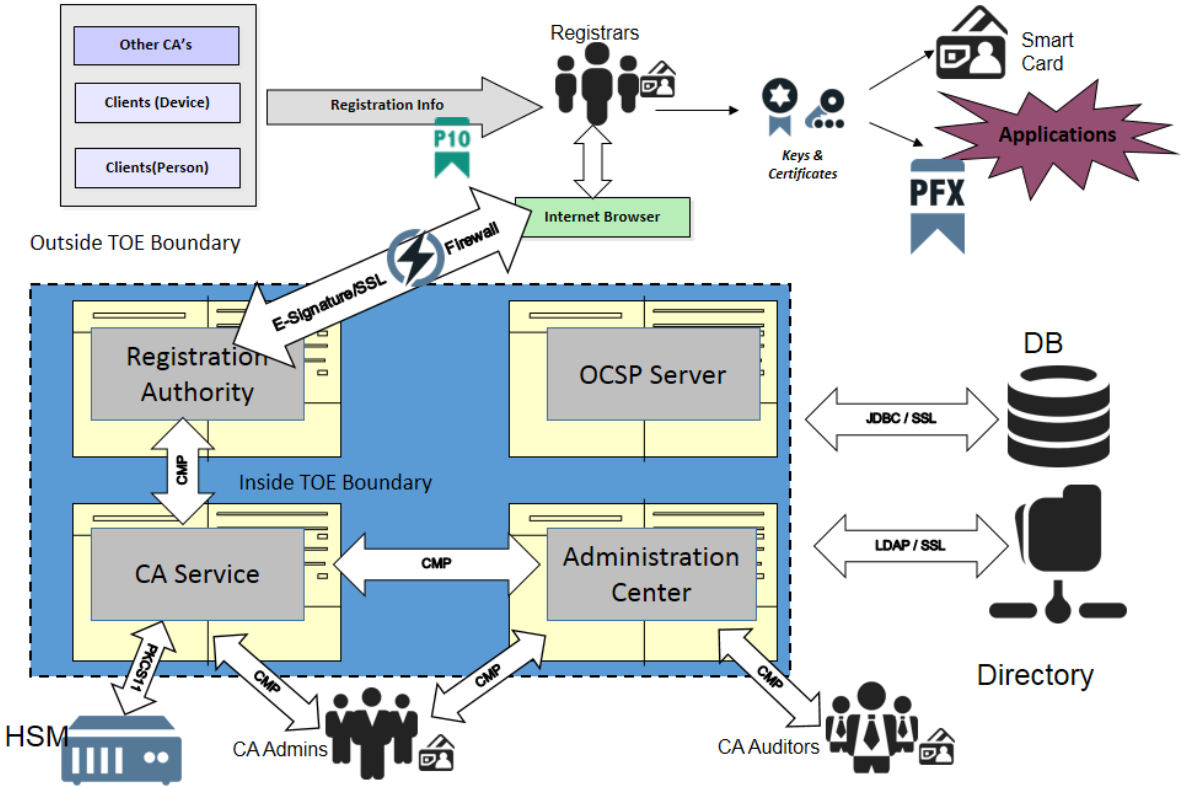

Figure 1 TOE Boundary

2.5 Documentation

These documents listed below are delivered to customer by the developer alongside the TOE:

Document Name	Version	Release Date
Security Target for ESYA v2.0	1.6	13.08.2015
Registration Authority User Guide	1.04	03.07.2015
Administration Center User Guide	1.7	03.07.2015
Installation Guide	1.6	03.07.2015

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families Common Criteria and Common Methodology; so the connections between the assurance families and the evaluation evidences has been established. The evaluation results are available in the final Evaluation Technical Report v2.0 of ESYA v2.0. It is concluded that the TOE supports EAL 4+ (ALC_FLR.2).

IT Product Testing is mainly realized in two parts:

1-Developer Testing:

- TOE Test Coverage: Developer has prepared TOE System Test Document according to the TOE Functional Specification documentation.
- TOE Test Depth: Developer has prepared TOE System Test Document according to the TOE Design documentation which include TSF subsystems and its interactions.
- TOE Functional Testing: Developer has made functional tests according to the test documentation. Test plans, test scenarios, expected test results and actual test results are in the test documentation.

2- Evaluator Testing:

The tests were performed with the product ESYA v2.0.

- Independent Testing: Evaluator has done a total of 36 sample independent tests. 14 of them are selected from developer`s test plans. The other 22 tests are evaluator`s independent tests. All of them are related to TOE security functions.
- Penetration Testing: Evaluator has done 22 penetration tests to find out if TOE`s vulnerabilities can be used for malicious purposes. The potential vulnerabilities and the penetration tests are in "TOE Security Functions Penetration Tests Scope" which is in Annex-D of the ETR and the penetration tests and their results are available in detail in the ETR document as well.

2.7 Evaluated Configuration

TOE	ESYA v2.0
Operating System	Windows 7+ (All versions) Windows 2003+ (All versions) ESYA v2.0 and Java installations must be 64-bit on 64-bit OSs. On this occasion; if ESYA is to be used on server machine after installation, Internet Explorer (64-bit) must be used as browser. While accessing remotely, if Java installed on local computer is 32-bit then any browser can be used. Also sunpkcs11.jar which is located under the installation folder, must be copied to \jre6\bin folder which is under where Java 64-bit installed at. (If Installation.exe is used then these steps are automatically done. On the other hand if any problem is encountered during installation, these steps must be done manually.)
Database Server	ORACLE 10i or higher or PostgreSQL 8.7 or higher UTF8 must be chosen as character set during the database installations.
Java Runtime	JRE 1.6.45
Crypto Hardware	At least one smart card reader,

	Hardware Security Module in which Certification Authority Keys will be stored, Admin smart card (at least 2 of them), Registrar smart card (at least one, after the Configuration of Administrator Center, it will be used during Registrar Definition which is explained in AC User Guide)
Internet Browser	Internet Explorer 9.0 or higher Mozilla Firefox 22.0 or higher Google Chrome 26.0 or higher Opera 26.0 or higher
Other Requirements	OS and pkcs11 drivers of smart card/HSM/card readers used.

2.8 Results of the Evaluation

The verdict for the CC Part 3 assurance component (according to EAL4+ (ALC_FLR.2) and the security target evaluation) are summarized in the following table:

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

2.9 Evaluator Comments / Recommendations

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of “ESYA v2.0” product, result of the evaluation, or the ETR.

3 SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:
Title: Security Target for Electronic Certificate Management Infrastructure v2.0
Version: 1.6
Date of Document: 13.08.2015

This Security Target describes the TOE, intended IT environment, security objectives, security requirements (for the TOE and IT environment), TOE security functions and all necessary rationale.

4 GLOSSARY

4.1-Acronyms

AC : Administration Center
ADV : Assurance of Development
AGD : Assurance of Guidance Documents
ALC : Assurance of Life Cycle
ASE : Assurance of Security Target Evaluation
ATE : Assurance of Tests Evaluation
AVA : Assurance of Vulnerability Analysis
BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
CC : Common Criteria (Ortak Kriterler)
CCCS : Common Criteria Certification Scheme (TSE)
CCRA : Common Criteria Recognition Arrangement
CCTL : Common Criteria Test Laboratory (OKTEM)
CEM :Common Evaluation Methodology
CMC : Configuration Management Capability
CMS : Configuration Management Scope
CMP : Certificate Management Protocol
CRL : Certificate Revocation List
DEL : Delivery
EAL : Evaluation Assurance Level
ESYA : Elektronik Sertifika Yönetim Altyapısı (TOE)
ETR : Evaluation Technical Report
HSM : Hardware Security Module
OCSP : Online Certificate Status Protocol
OKTEM : Ortak Kriterler Test Merkezi (CCTL)
OSP : Organisational Security Policy
PP : Protection Profile
RA : Registration Authority
SAR : Security Assurance Requirements
SFR : Security Functional Requirements
ST : Security Target
STCD :Software Test and Certification Department
TOE : Target of Evaluation
TSF : TOE Security Function
TSFI : TSF Interface

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012

[3] BTBD-03-01-TL-01 Certification Report Preparation Instructions, Rel.Date: August,4,2015

[4] ESYA v2.0 Registration Authority User Guide v1.04 Rel. Date: 03.07.2015

[5] ESYA v2.0 Administration Center User Guide v1.7 Rel. Date: 03.07.2015

[6] ESYA v2.0 Installation Guide v1.6 Rel. Date: 03.07.2015

[7] ETR v2.0 of ESYA v2.0 Rel. Date: 18.08.2015 (Document code: DTR 38 TR 02)