COMMON CRITERIA RECOGNITION ARRANGEMENT
FOR COMPONENTS UP TO EAL 4

Certification Report

EAL 4+ Evaluation of

TÜBİTAK UEKAE
ELECTRONIC CERTIFICATE MANAGEMENT INFRASTRUCTURE v1.0
(ESYA v1.0)

issued by

Turkish Standards Institution
Common Criteria Certification Scheme

Date : **01 March 2010**
Pages : **39**
Certification Report
Number : **14.10.01/ 10-105, r1**

This page left blank on purpose.

----- o -----

TABLE OF CONTENTS:

This page left blank on purpose.

----- o -----

CERTIFICATION REPORT

The Certification Report is drawn up to submit the Certification Committee 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 PCC Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

1. INTRODUCTION

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 with respect to that standard by the Turkish Accreditation Agency (TÜRKAK), the national accreditation body in Turkey. The evaluation and tests related with the concerned product have been performed by TÜBİTAK-UEKAE Common Criteria Test Center (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 ESYA - Electronic Certificate Management Infrastructure (product version: v1.0) whose evaluation was completed on 26.02.2010 and whose evaluation technical report was drawn up by OKTEM (as CCTL), and with the Security Target document with version no. 1.22 of the relevant product.

2. GLOSSARY

CCCS: Common Criteria Certification Scheme

CCTL: Common Criteria Test Laboratory

CRL: Certification Revocation List

ESYA: Elektronik Sertifika Yönetim Altyapısı (Electronic Certificate Management Infrastructure)

ETR: Evaluation Technical Report

IT: Information Technology

OKTEM: Common Criteria Test Center (as CCTL)

PCC: Product Certification Center

ST: Security Target

TOE: Target of Evaluation

TÜBİTAK: Turkish Scientific and Technological Research Council

TÜRKAK: Turkish Accreditation Agency

UEKAE: National Electronics and Cryptology Research Institute

CMP: Certificate Management Protocol

CA: Certification Authority

3. EXECUTIVE SUMMARY

Evaluated IT product name:

Electronic Certificate Management Infrastructure - Elektronik Sertifika Yönetim Altyapısı (ESYA)

IT Product version:

Version 1.0

Developer`s Name:

TÜBİTAK UEKAE MA3 Project Group

Name of CCTL :

TÜBİTAK UEKAE OKTEM Common Criteria Test Center

Completion date of evaluation :

26.02.2010

Common Criteria Standard version :

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 3, July 2009
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 3, July 2009, extended.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009, conformant.

Common Criteria Evaluation Method version :

- Common Methodology for Information Technology Security Evaluation Version 3.1 revision3, July 2009

Short summary of the Report:

1) **Assurance Package :**
EAL 4+ (ALC_FLR.2)

2) Functionality :

ESYA v1.0 (TOE) is an X.509 certificate generation and management system software. TOE and its operational environment provide 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.

In TOE three different roles are defined:

Administrator

Administrators administrate Certification Authority Services and Administration Center.

Registrar

Registrars register and manage the end users and device information through the Registration Authority application.

Auditor

Auditors review the audit logs and create reports using the Administration Center application.

So the components that are included within TOE boundary are:

- Certification Authority Services
- Administration Center
- Registration Authority

The detailed information about the functionality can be found in part 1.4 of Security Target document.

3) Summary of Threats and Organizational Security Policies (OSPs) addressed by the evaluated IT product:

The threats are organized in three categories:

- **Threats countered by TOE:**

T. Sender denies sending information : The sender (authorized users) of a message denies sending the message to avoid accountability for sending the message and for subsequent action or inaction.

- **Threats countered by TOE Operational Environment:**

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

- **Threats countered by both TOE and TOE Operational Environment:**

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

T. Administrators, Registrars and Auditors commit errors: An Administrator, Registrar or Auditor commits errors that change the intended security policy of the TOE and its operational environment.

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

T. Malicious code exploitation : A distant hacker downloads and executes malicious code, which causes abnormal processes that violate the integrity, availability, or confidentiality of the system assets. The malicious code is not a self running code but it is executed through a triggering event.

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. 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.

T. Hacker gains access : A distant 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. Modification of private/secret keys : A secret/private key is modified by a distant hacker so that invalid certificates can be issued

T. Disclosure of private and secret keys : A private or secret key is improperly disclosed by a distant hacker due to insufficient security measures or errors committed by the Administrators, Registrars or Auditors so that fake certificates can be issued by unauthorized people.

- **Organizational Security Policies (OSPs)**

P. Authorized use of information : Information shall be used only for its authorized purpose(s). Authorization and authentication management of the TOE users will be managed according to the TOE Access Control Policy.

P. Cryptography and secure storage of cryptographic assets : FIPS-approved or NIST-recommended cryptographic algorithms and devices shall be used to perform all cryptographic operations.

4) Special Configuration Requirements:

Special configuration requirements are presented in the following Table 1:

Operating System	Windows 2000 (all versions) at least Service Pack 3 Windows 2003 (all versions) (The recommended OS for the TOE is Windows 2003 which is certified with Common Criteria EAL 4 level.)
Database Server	ORACLE 10i or upper (All the infrastructure and end user data is stored in the database)
Java Runtime	JRE 1.6.x and upper (It's a java application server which runs the Registration Authority. It can be one of the COTS java application servers like Apache Tomcat, Sun ONE etc)
Crypto Hardware	At least one smart card reader At least 2 smart cards for Administrators At least 2 smart cards for Registrars
Directory Server	There must be an accessible LDAP compatible directory server in order to publish certificates, CRLs on network. This server can be the types below: • Injoin Directory Server (Critical Path) • iPlanet (Netscape) • DirX (Siemens) • Fedora (Red Hat) • Microsoft Active Directory, Microsoft ADA vb.
Hardware	Certification Authority Services and Administration Center • Windows 2003 R2 Service Pack 2 x86 32bit Pentium III 800 MHz processor • 512 MB RAM and minimum 300 MB disk space Registration Authority • Windows 2003 R2 Service Pack 2 x86

	32bit Pentium III 800 MHz processor • 512 MB RAM and minimum 1 GB disk space

Table 1 Special configuration requirements

5) Assumptions about the Operating Environment:

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

A. Physical Protection: The TOE and the operational environment are protected from physical attack that might compromise IT security.

A. Operating System: The operating system has been selected to provide the functions required by the TOE.

6) Disclaimers:

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 3, using Common Methodology for IT Products Evaluation, version 3.1, revision 3. 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.

4. IDENTIFICATION

ESYA (Electronic Certificate Management Infrastructure) v1.0 (TOE) is an X.509 certificate generation and management system software.

ESYA v1.0 (TOE) is an X.509 certificate generation and management system software. TOE and its operational environment provides privacy, access control, integrity, confidentiality, authentication and no- 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.

In TOE three different roles are defined:

- **Administrator**

Administrators administrate 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 log-on to the Certification Authority Services and Administration Center applications.

- **Registrar**

Registrars register and manage the end users and device information through the Registration

Authority application. They also create requests to the Certification Authority Services for issuing or revoking certificates. Registrars are not entitled to run all the services offered by the Registration Authority. The access control of the services for the registrars is configurable from the Administration Center. Registrars use smartcards which contain signature, encryption key pairs and the corresponding registrar certificates issued by the CA in order to log-on to the Registration Authority application.

- **Auditor**

Auditors review the audit logs and create reports using the Administration Center application. Auditors use smartcards which contain signature, encryption key pairs and the corresponding auditor certificates issued by the CA in order to log-on to the Administration Center application.

TOE Boundary

The components that are included within TOE boundary are:

- Certification Authority Services
- Administration Center
- Registration Authority

The servers are not parts of the TOE. They are environmental components. TOE is completely software, it does not include any hardware or firmware components.

Certification Authority Services

Certification Authority Services

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

Certification Service

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

CRL Service

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

Archive Service

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

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).

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

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 and validating end user and device information for certificate generation
- Access through a web based interface for registrars
- Management of end user, device information

- Requesting certificate from the certification server for end users and device information.
- A web based interface for self requesting certificate for the end users
- Request for revoking or placing a certificate on hold.

TOE Operational Environment

The components that are outside the TOE boundary are given below. Also the justifications for exclusion are also explained.

Database

All the infrastructure and end user data is stored in the database. The following data is stored as encrypted.

- Symmetric key for DB table row signature
- Directory user's password
- End user encryption certificate private keys

This security target has no claims regarding the internal security of the database. The confidentiality and integrity of the sensitive data stored in the database is provided by TOE which uses the cryptographic functions from the environment. In addition, this document also has no claims regarding the basic database functionality. None of the database functionality is matched with the security functionality requirement.

Directory

TOE supports LDAP compatible directories. Public certificates of users and certificate revocation lists are written by the Certificate and CRL services to the directory.

This document has no claims regarding the internal security of the directory. None of the basic directory functionality is matched with the security functionality requirement.

Java Application Server

It's a java application server which runs the Registration Authority. It can be one of the COTS java application servers like Apache Tomcat, Sun ONE etc.

This document has no claims regarding the internal security of the java application server.

Hardware and Operating System Platform

- **Operating System:** It is assumed that OS works correctly. The recommended OS for the TOE is Windows 2003 which is certified with Common Criteria EAL 4 level.
- **Hardware Independence:** TOE is optimized to execute any x86-based machines, regardless of the hardware vendor. TOE can run on the hardware platform which meets the following minimum requirements.

▪ **Certification Authority Services and Administration Center**

- Windows 2003 R2 Service Pack 2 x86 32bit Pentium III 800 MHz processor
- 512 MB RAM and minimum 300 MB disk space

▪ **Registration Authority**

- Windows 2003 R2 Service Pack 2 x86 32bit Pentium III 800 MHz processor
- 512 MB RAM and minimum 1 GB disk space

Cryptographic Modules

HSM

FIPS 140-2 level 3 validated hardware cryptographic modules must be used for the following cryptographic functions used by the TOE.

- Certificate Signing
- CRL Signing
- Encryption private key decryption for key recovery

Software Cryptographic Module

The following cryptographic functions are performed in the software cryptographic module. This module is bundled with the TOE software but it's not a part of the TOE.

- Key Generation
- Asymmetric Encryption
- Signature Verification
- Symmetric Encryption/Decryption
- Hash generation
- MACs

Smart Cards

At least CC EAL 4 validated smartcards are used for identification and authentication of Administrators, Registrars and Auditors.

5. SECURITY POLICY

TOE and its operational environment provide privacy, access control, integrity, confidentiality, authentication and non-repudiation services. TOE Major Security Features are listed below:

TOE Major Security 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;
- 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, self tests and audit logs;
- The data transmitted between the TOE and remote users are protected against modification and disclosure.

TOE enforces the following **security policies** in conjunction with the IT environment, these are from chapter 7 of Security Target, the summary of IT Security Functions:

IT Security Functions:

- **Security Audit Policy:** Audit Data Generation, Accountability of Users, Audit Data Selection, Audit Data Protection, Prevention of Audit Data Loss, Query of Audit Logs.
- **Roles Policy:** Role Definition(Administrator, Registrar,Auditor), Management of Security Functions Behaviour, Seperation of Roles**.**

- **Scope of Policy and Access Rules Policy**
- **Identification and Authentication Policy**
- **Remote Data Entry and Export Policy**: Enforced Proof of Origin and Verification of Origin, Protection of Data Communications between CA Services and Registration Authority, Trusted Channel.
- **Certificate Management Policy**: Certificate Generation, Certificate Status Export, Certificate Profile Management.
- **Certificate Revocation Policy:** CRL Profile Management, CRL Validation.
- **Key Management Policy:** Private Key Protection, Public Key Protection.

Security Functional Requirements:

Additionally in ESYA v1.0 Security Target chapter 6 there are **Security Functional Requirements** that conclude Security Policy. A summary of the SFRs for the TOE and IT environment are included in the tables below. Table 2 presents **TOE Functional Security Requirements:**

Security Requirement		Component
Security Audit (FAU)	Audit data generation	FAU_GEN.1
	User identity association	FAU_GEN.2
	Selective audit	FAU_SEL.1
	Protected audit trail storage	FAU_STG.1
	Prevention of audit data loss	FAU_STG.4
Communication (FCO)	Enforced proof of origin and verification of Remote Data Entry and Export	FCO_NRO_TOE.3
	Advanced verification of origin Remote Data Entry and Export	FCO_NRO_TOE.4
User Data Protection (FDP)	Subset access control	FDP_ACC.1
	Security attribute based access control	FDP_ACF.1
	User private key confidentiality protection	FDP_ACF_TOE.2
	Certificate Generation	FDP_TOE_CER.1
	Certificate Revocation	FDP_TOE_CRL.1
	Certificate status export	FDP_TOE_CSE.1
	Extended user private and secret key export	FDP_ETC_TOE.5
	Basic internal transfer protection (Iteration 1 and 2)	FDP_ITT.1
	Stored public key integrity monitoring and action	FDP_SDI_TOE.3
	Basic data exchange confidentiality	FDP_UCT.1
Identification and Authentication (FIA)	User attribute definition	FIA_ATD.1
	Timing of authentication	FIA_UAU.1
	Timing of identification	FIA_UID.1

	User-subject binding	FIA_USB.1
Security Management (FMT)	Specification of Management Functions	FMT_SMF.1
	Management of security functions behavior	FMT_MOF.1
	Extended certificate profile management	FMT_MOF_TOE.3
	Extended certificate revocation list profile management	FMT_MOF_TOE.5
	Management of security attributes	FMT_MSA.1
	Static attribute initialization	FMT_MSA.3
	Management of TSF data	FMT_MTD.1
	TSF secret key confidentiality protection	FMT_MTD_TOE.5
	Extended TSF private and secret key export	FMT_MTD_TOE.7
	Restrictions on security roles	FMT_SMR.2
Protection of the TSF (FPT)	Audit log signing event	FPT_TOE_TSP.1
	Inter-TSF confidentiality during transmission	FPT_ITC.1
	Basic internal TSF data transfer protection (Iteration 1 and 2)	FPT_ITT.1

Table 2 TOE Functional Security Requirements

Table 3 presents **IT Environment Functional Security Requirements:**

Security Requirement		**Component**
Cryptographic Support (FCS)	Cryptographic key generation	FCS_CKM.1
	Cryptographic key destruction	FCS_CKM.4
	Cryptographic operation	FCS_COP.1
Protection of the TSF (FPT)	Reliable time stamps	FPT_STM.1
Trusted Path/Channel (FTP)	Trusted path	FTP_TRP.1

Table 3 IT Environment Functional Security Requirements

6. ARCHITECTURAL INFORMATION

TOE and its environment are seen in the following figure.

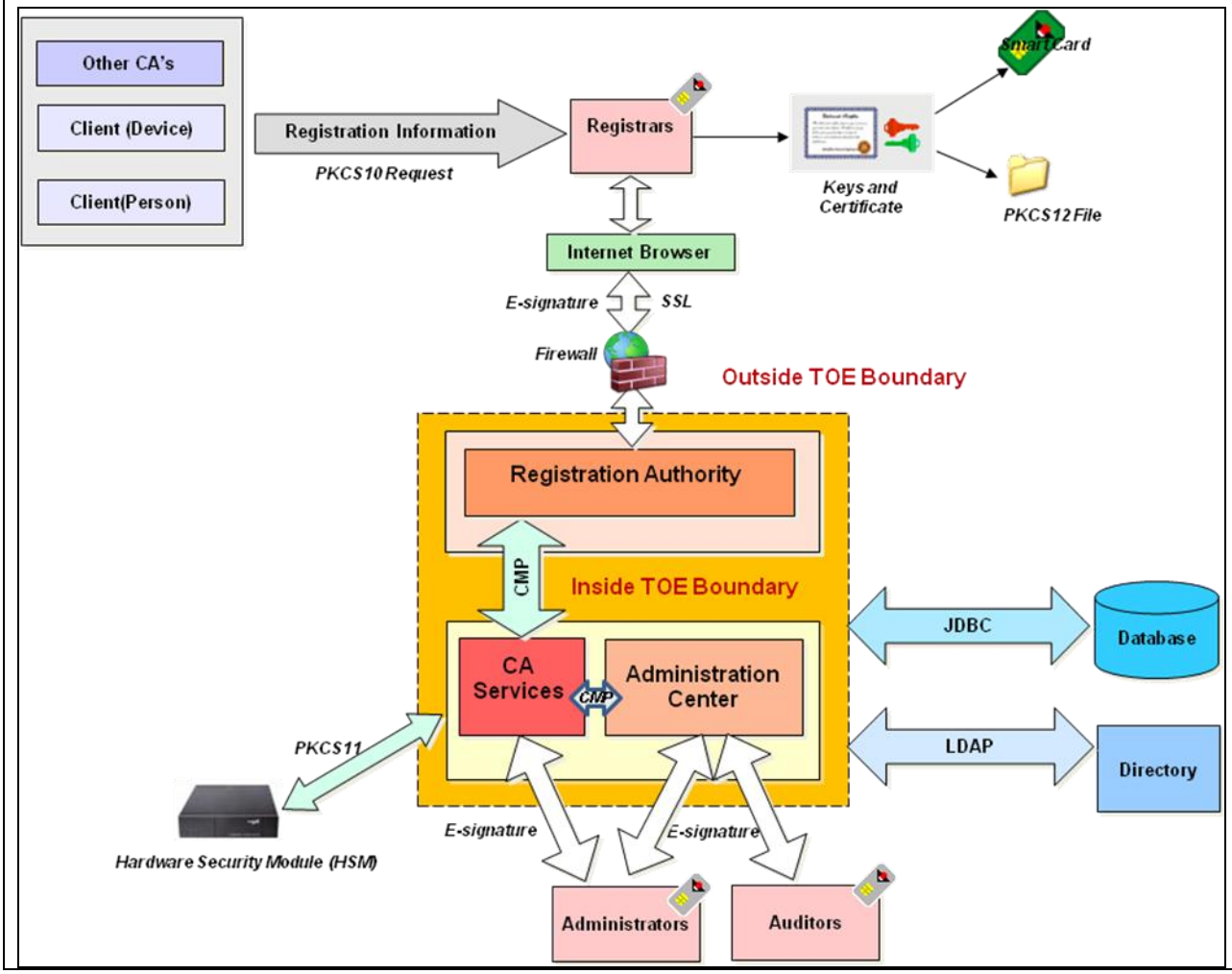

Figure 1 TOE Boundary and environmental components

TOE boundary is indicated in Figure 1. The components that are included within TOE boundary are:

- Certification Authority Services
- Administration Center
- Registration Authority

- Detailed architectural information of ESYA has been presented under the "IDENTIFICATION" subtitle of this Certification Report.

Note: The servers, which are shown inside the TOE boundary at Figure 1, are not parts of the TOE. They are environmental components. TOE is completely software, it does not include any hardware or firmware components.

In Figure 2 which is from ESYA v1.0 Detailed Design and Security Architecture Document, there is the summary of ESYA subsystems and its modules. These modules make the subsystems` infrastructure. The detailed explanation of the subsystems, modules and the Security Functions of TOE`s modules are in the **Design Document** of ESYA v1.0.

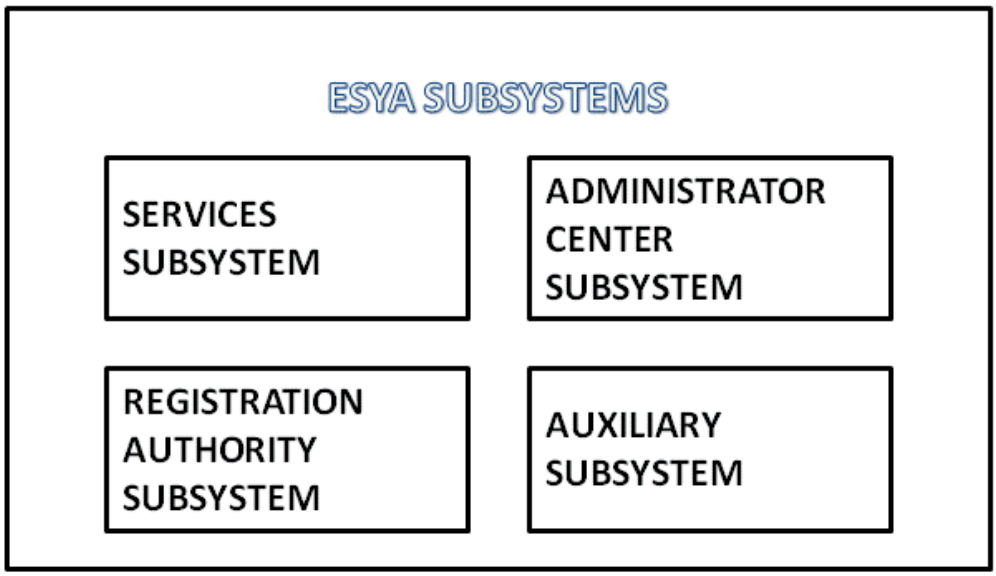

Figure2 TOE Subsystems

Also how the target Security Functions are verified by subsystems and modules and its rationality are explained in ESYA v1.0 Security Target document.

7. ASSUMPTIONS AND CLARIFICATION OF SCOPE

TOE is explained in detail under the subtitle "ARCHITECTURAL EXPLANATION" part of this report, TOE is only software,

The servers, which are shown inside the TOE boundary at Figure 1, are not parts of the TOE. They are environmental components. TOE is completely software, it does not include any hardware or firmware components so they are outside the scope of Common Criteria evaluation.

7.1 Usage Assumptions

Usage assumptions related to the secure operation of the TOE are given in the following Table 4:

A. Auditors Review Audit Logs	Audit logs must be reviewed by the Auditors at least once a week.
A. Authentication Data Management	An authentication data management policy is enforced to ensure that authorized users change their authentication data at least once a month with minimum 6 digit numbers.
A. Competent Administrators, Officers and Auditors	Competent Administrators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains.
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	Since authorized users do not intentionally perform hostile actions, Officers and Auditors notify Administrators of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
A. Cooperative Users	TOE users need to accomplish some task or group of tasks that require a secure IT environment. The TOE users require access to

	at least some of the information managed by the TOE and are expected to act in a cooperative manner.

Table 4 Usage Assumptions

7.2 Environmental Assumptions

The environmental assumptions listed in the following Table 5, are required to ensure the security of the TOE.

A. Communications Protection	The system is adequately physically protected against loss of communications i.e., availability of communications.
A. Physical Protection	The TOE and the operational environment are protected from physical attack that might compromise IT security.
A. Operating System	The operating system has been selected to provide the functions required by the TOE.

Table 5 Environmental Assumptions

7.3 Clarification of Scope

TOE "ESYA v1.0" is evaluated at certified at EAL 4+ (ALC_FLR.2) under the assumption that "Competent and innocuous Administrators, Officers and Auditors will be assigned to manage the TOE and the security of the information it contains and the authorized users will not intentionally perform hostile actions". In the User Guide, the role of the registrar is specified for this purpose. In ST, the event of "malicious and incompetent users" are countered by assumptions so only under these assumptions TOE can operate correctly.

Under normal conditions; there are no threats which TOE must counter but did not; however Operational Environment and Organizational Policies has countered. Information about threats that are countered by TOE and Operational Environmental are stated in the Security Target document.

8. DOCUMENTATION

The following is a list of the end-user documentation:

TOE documentation:

TOE – Elektronik Sertifika Yönetim Altyapısı (ESYA) –Electronic Certificate Management Infrastructure
Version Number and Date: 1.0, 12.02.2010

ESYA v1.0 Security Target
Version Number and Date: 1.22, 15.02.2010

ST Lite- ESYA v1.0 Security Target Lite (public)
Version Number and Date: 1.0 - December 07, 2010

ESYA v1.0 Usage Guide document
Version Number and Date: 1.11 – 22.02.2010

ESYA v1.0 Installation Guide Document
Version Number and Date: 1.05 – 12.02.2010

ESYA v1.0 Flaw Remediation Client Guide Document
Version Number and Date: 4.0 – 15.02.2010

Guides about Environmental units:

ADAM SP1 Installation Document for ESYA v1.0
Version Number and Date: 3 – 15.02.2010

Critical Path IDS 3.1 Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Netscape IPlanet 5.0 Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 netHSM Installation and Usage Guide Document
Version Number and Date: 5.5 – 21.09.2005

ESYA v1.0 OpenBSD 4.6 Installation Guide Document

ESYA v1.0 OpenBSD 4.6 Packet Filtration Document

ESYA v1.0 Oracle 10gR2 32 bite Installation Guide Document
Version Number and Date: November 2007

ESYA v1.0 Oracle Database Composing Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Plan and Configuration Guide Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows 2000, XP, 2003, 2003 R2X86 Smart Card Reader Installation Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows 2003 R2X86 Installation Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows Oracle 10.2.0.3 Installation Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows AKİS Smart Card Installation Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows Datakey/IKey Smart Card Installation Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows JAVA 1.6.16 Installation Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows Sunone Web Server 6 Installation Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows Sunone Web Server 7 Installation Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows TOMCAT 5.x Installation Document
Version Number and Date: 2 – 15.02.2010

ESYA v1.0 Windows TOMCAT 6.x Installation Document
Version Number and Date: 2 – 15.02.2010

9. IT PRODUCT TESTING

During the evaluation, all evaluation evidences of TOE were delivered and transfered completely to CCTL by the developers. All the delivered evaluation evidences which include software, documents, etc are mapped to the assurance families of Common Criteria and Common Methodology; so the connections between the assurance famillies and the evaluation evidences has been established. This is shown in detail in ST document Table 0.1 (Assurance measures). The evaluation results are available in the Evaluation Technical Report (ETR) of ESYA v1.0.

It is concluded that the TOE supports EAL 4 +(ALC_FLR.2). Table 3 under the subtitle "RESULTS AND EVALUATION" of this certification report , there are 25 assurance families which are all evaluated with the methods detailed in the ETR.

IT Product Testing is mainly realized in two parts:

1) **Developer Testing :**

- **TOE Test Coverage**: Developer has prepared TOE Analysis of Coverage Document according to the TOE Functional Specification documentation.
- **TOE Test Depth:** Developer has prepared TOE Analysis of Depth of Testing 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 :**

- **Independent Testing:** Evaluator has done a total of 19 sample independent tests. 16 of them are selected from developer`s test plan which include a total of 42 tests. The other 3 tests are evaluator`s independent tests. All of them are related to TOE security functions.

- **Penetration Testing:** Evaluator has done 29 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-C of the ETR and the penetration tests and their results are available in detail in the ETR document as well.

The assurance classes related to the developer and evaluator tests are ATE and AVA classes:

Class ATE: The purpose of the **Tests Assurance Class** is to identify if TOE behaves consistently with the TOE Security Functional Requirements as it is mentioned in the TOE Design Documentation and the Security Target. This subject can be concluded by determining if the developer prepared Test Coverage and Depth documents according to the Functional Specifications and the Detailed Design document. Then developer should have tested TSF according to these Test Coverage and Depth documents. The evaluator first checks the consistency of the Test Coverage and Depth documents with ST and Functional Specification documents, then the evaluator selects some of the developer`s security functional tests and repeats them. Hence a subset of the TSF is tested independently by the evaluator to complete the evaluation of this assurance class.

The following families are within the scope of the Test assurance class:

ATE_COV.2: Coverage

ATE_DPT.1: Depth

ATE_FUN.1: Functional Tests

ATE_IND.2: Independent Testing

Class AVA: The purpose of the **Vulnerability Assessment class** is to find out whether TOE`s vulnerabilities can be used for malicious purposes or not. This identification is done by the evaluator`s penetration tests. The scope of penetration tests about potential vulnerabilities is defined in "TOE Security Functions Penetration Tests Scope" which is in Annex-C of the ETR document.

For the product ESYA v1.0, evaluator has done 29 penetration tests. These tests, their results and the mapping information between the test and the related TOE`s subsystem, module, interface and security function are available in the ETR document.

AVA_VAN.3 is within the scope of the AVA class.

The result of AVA_VAN.3 evaluation is given below:

- It is determined that TOE, in its operational environment, is resistant to an attacker possessing **"Enhanced-Basic"** attack potential.
- For the product ESYA v1.0, **there are no exploitable vulnerabilities** in the scope of the assumptions in ST (Competent Administrators, Officers and Auditors will be assigned to manage the TOE and the information it contains and authorized users will not intentionally perform hostile actions).

Table 6 presents a summary of the work done about ATE and AVA classes:

CC Assurance Component		Evaluation Evidence	Related Developer-Evaluator Actions
ATE_COV.2	Analysis of coverage	• ESYA v1.0 Test Coverage Chart Document • ESYA v1.0 Test Documents • ESYA v1.0 ST • ESYA v1.0 Functional Specification document	**Developer action:** Developer has derived Test Coverage Chart document and Test document from the TOE Functional Specification and ST documents in order to test all TSFIs. **Evaluator action:** Evaluator has checked the Test Coverage document and Test document in order to find out whether the developer has tested all of the TSFIs in the functional specification or not.
ATE_DPT.1	Testing: basic design	• ESYA v1.0 Test Depth Chart Document • ESYA v1.0 Test Documents	**Developer action:** Developer has derived Test Depth Chart

		• ESYA v1.0 ST • ESYA v1.0 Functional Specification document • ESYA v1.0 Detailed Design and Security Architecture Document	Document and Test document from the TOE design documentation in order to test all TSF subsystems. **Evaluator action:** Evaluator has checked the Test Depth Chart document and Test document in order to find out whether the developer has tested all of the TSF subsystems or not.
ATE_FUN.1	Functional testing	• ESYA v1.0 Test Documents • ESYA v1.0 ST • ESYA v1.0 Functional Specification document	**Developer action:** Developer has made functional tests on TOE and recorded the results of functional tests. Test plans, test scenarios, expected test results and actual test results are all in the Test documentation. **Evaluator action:** Evaluator has checked Test documentation to find out if the developer has performed and recorded the results of functional tests properly.
ATE_IND.2	Independent testing – sample	• TOE – ESYA– Electronic Certificate Management Infrastructure v 1.0 • ESYA v1.0 Test Documents • ESYA v1.0 ST • ESYA v1.0 Functional Specification document • ESYA v1.0 Usage Guide document • ESYA v1.0 Installation	**Evaluator action.** Evaluator has made a total of 19 sample independent tests. 16 of these tests are selected from developer`s test plan which include a total of 42 tests. The other 3 tests are evaluator`s

		Guide Document • ESYA v1.0 Detailed Design and Security Architecture Document • ESYA v1.0 Configuration Management Plan • ESYA v1.0 Test Documents	independent tests. All of them are related to TOE security functions.
AVA_VAN.3	Focused vulnerability analysis	• TOE – ESYA– Electronic Certificate Management Infrastructure v 1.0 • ESYA v1.0 Test Documents • ESYA v1.0 ST • ESYA v1.0 Functional Specification document • ESYA v1.0 Usage Guide document • ESYA v1.0 Installation Guide Document • ESYA v1.0 Detailed Design and Security Architecture Document • ESYA v1.0 Configuration Management Plan • ESYA v1.0 Test Documents	**Evaluator action**. Evaluator has performed 29 penetration-vulnerability tests on the TOE. The scope of penetration tests about potential vulnerabilities is defined in "TOE Security Functions Penetration Tests Scope" which is in Annex-C of the ETR document.

Table 6: Summary of the work done about ATE and AVA classes

As a result of the evaluation , the TOE was found to fulfill the Common Criteria requirements for each of 25 assurance families and thus to provide the assurance level EAL 4+ (ALC_FLR.2)

10. EVALUATED CONFIGURATION

During the evaluation; the configuration of evaluation evidences which are composed of Software source code, Common Criteria documents, sustenance document and guides are shown below:

Evidences related to TOE:
TOE – Elektronik Sertifika Yönetim Altyapısı (ESYA) –Electronic Certificate Management Infrastructure
Version Number and Date: 1.0 – 12.02.2010

ESYA v1.0 Source Code
Version Number and Date: 1.0 –12.02.2010

ESYA v1.0 Detailed Design and Security Architecture Document
Version Number and Date: 08 –15.02 2010

ESYA v1.0 Functional Specification Document
Version Number and Date: 10 –15.02.2010

ESYA v1.0 Flaw Remediation Method Document
Version Number and Date: 4.0 – 15.02.2010

ESYA v1.0 Flaw Remediation Client Guide Document
Version Number and Date: 4.0 – 15.02.2010

ESYA v1.0 Delivery Procedures Document
Version Number and Date: 5.0 – 15.02.2010

ESYA v1.0 Configuration Management Plan
Version Number and Date: 07 – 15.02.2010

ESYA v1.0 Development Environment Security and Development Tools
Version Number and Date: 06 – 15.02.2010

ESYA v1.0 Life Cycle Document
Version Number and Date: 4.0 – 15.02.2010

Configuration Evidences
Version Date: 30.12.2009

ST- ESYA v1.0 Security Target
Version Number and Date: 1.22 - February 15, 2010

ST Lite- ESYA v1.0 Security Target Lite (public)
Version Number and Date: 1.0 - December 07, 2010

ESYA v1.0 Test Coverage Chart Document
Version Number and Date: 5 – 15.02.2010

ESYA v1.0 Test Depth Chart Document
Version Number and Date: 4 – 15.02.2010

ESYA v1.0 Test Documents
Version Number and Date: 5 – 12.02.2010

ESYA v1.0 Usage Guide document
Version Number and Date: 1.11 – 22.02.2010

ESYA v1.0 Installation Guide Document
Version Number and Date: 1.05 – 12.02.2010

Evidences related to Operational Environment:

ADAM SP1 Installation Document for ESYA v1.0
Version Number and Date: 3 – 15.02.2010

Critical Path IDS 3.1 Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Netscape IPlanet 5.0 Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

ESYA netHSM Installation and Usage Guide Document
Version Number and Date: 5.5 – 21.09.2005

ESYA OpenBSD 4.6 Installation Guide Document

ESYA OpenBSD 4.6 Packet Filtration Document

ESYA Oracle 10gR2 32 bite Installation Guide Document
Version Number and Date: November 2007

Oracle Database Composing Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Plan and Configuration Guide Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Windows 2000, XP, 2003, 2003 R2X86 Smart Card Reader Installation Document For ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Windows 2003 R2X86 Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Windows Oracle 10.2.0.3 Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Windows AKİS Smart Card Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Windows Datakey/IKey Smart Card Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Windows JAVA 1.6.16 Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Windows Sunone Web Server 6 Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Windows Sunone Web Server 7 Installation Document for ESYA v1.0
Versiyon Numarası ve Tarihi: 2 – 15.02.2010

Windows TOMCAT 5.x Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

Windows TOMCAT 6.x Installation Document for ESYA v1.0
Version Number and Date: 2 – 15.02.2010

11. RESULTS OF THE EVALUATION

Table 7 below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_FLR.2: Flaw reporting procedures.

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

Table 7 TOE Security Assurance Requirements of EAL 4+ (ALC_FLR.2)

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE ESYA

v1.0 the result of the assessment of all evaluation tasks are "**Pass**".

Results of the evaluation:

ESYA v1.0 product was found to fulfill the Common Criteria requirements for each of 25 assurance families and provide the assurance level EAL 4+ (ALC_FLR.2).

This result shows that **TOE is resistant againist the "ENHANCED-BASIC'' level attack potential** and it countervails the claims of the functional and assurance requirements which are defined in ST document.

There is no residual vulnerability (vulnerabilities can be used as evil actions by the hostile entities who have MEDIUM or HIGH level attack potential), that they do not affect the evaluation result, found by CCTL under the conditions defined by the evaluation evidences and developer claims.

12. EVALUATOR COMMENTS/ RECOMMENDATIONS

No recommendations or comments have been communicated to CCCS by the evaluators related to the evaluation process of ESYA v1.0 product, result of the evaluation, or the ETR.

13. CERTIFICATION AUTHORITY COMMENTS/ RECOMMENDATIONS

The certifier has no comments or recommendations related to the evaluation process of ESYA v1.0 product, result of the evaluation, or the ETR.

14.SECURITY TARGET

Information about the Security Target document associated with this certification report is as follows:

Name of Document **:** ESYA v1.0 Security Target
Version No. **:** 1.22
Date of Document **:** 15 February 2010

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.

15. BIBLIOGRAPHY

1. PCC-03-WI-04 CERTIFICATION REPORT PREPARATION INSTRUCTIONS, Version 1.0.

2. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

3. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

4. ESYA (Electronic Certificate Management Infrastructure ECMI) (product version: v 1.0) Security Target v.1.22, February 15, 2010.

5. Evaluation Technical Report (Document Code: DTR 07 TR 01), February 26, 2010.

16. APPENDICES

There is no additional information which is inappropriate for reference in other sections.

PREPARED BY

INSPECTION EXPERT	CERTIFICATION EXPERT
Name, Last Name: Mariye Umay AKKAYA	**Name, Last Name:** Merve Hatice KARATAŞ
Title: CCCS Inspection Expert	**Title:** CCCS Certification Expert
Signature:	**Signature:**

APPROVED BY

Name, Last Name: Cengiz OĞUZ
Title: Electrotechnic Sector Certification Manager
Signature: