ESYA
Certification Authority
Technical Specifications

Operating System

Windows 2003 +, Linux

Hardware Requirements

- Intel/AMD processor
- Minimum 2 GB RAM
- 500 MB free disk space

Software Requirements

- Oracle 10g+ or Postgre SQL 8.1+ database
- Java JDK 1.6+
- Any server supporting with servlet support like TomCat

Supported Standards

- X.509 v3 Certificates, X.509 v2 Certificate Revocation Lists (CRL)
- Online Certificate Status Protocol (OCSP)
- PKIX Certificate Management Protocol (CMP)
- LDAP Protocol

Directory Services

- Automatic publishment of the certificates in a directory
- Compatible with all X.500 directory servers (Fedora Directory Server, Active Directory etc.)

PKI Services

- X.509 v3 certificate creation
- X.509 v2 certificate revocation list creation
- Creation and back up of encryption keys at server
- Key Recovery and Update
- Unlimited number of CAs under Root Certificate Authority in a desired hierarchy.
- Cross certification support

Certificate Types

Creation of different types of X.509v3 certificates by using certificate templates, such as;

- Qualified Certificates
- SSL, VPN
- Windows Smartcard Logon Certificate, Windows Domain Controller Certificate

Cryptographic Features

- RSA algorithm (1024, 2048, 4096)
- ECDSA algorithm (163, 192, 256, 368, 431, 512)
- SHA1, SHA256, SHA384, SHA512 hash algorithms

Cryptographic Hardware Support

- PKCS 11 compliant smartcards and tokens
- "M of N" key sharing
- HSM (Hardware Security Module) support

Proprietary Features

- All products are developed by TÜBİTAK BİLGEM UEKAE
- Quick on-demand customization.

TÜBİTAK
BİLGEM

Electronic Certificate Management Infrastructure

ESYA Certification Authority

Electronic Certificates are one of the most important components of Public Key Infrastructure (PKI) , which is a technology built on asymmetric cryptology. Certification Authority (CA) and other supporting software are required in order to create electronic certificates. CAs creates certificates for other CAs, users , servers and devices.

ESYA Certification Authority, supports industrial electronic certificates standards (X.509, CVC etc.) and provides certificate service providers (CSPs) with all services required throughout the lifecycle of electronic certificates (creation, renewal, revocation, etc.) via a user-friendly interface.

Solutions

Certificate and Key Generation

For all software and hardware products which make use of cryptographic keys and certificates, generation and management of keys and certificates

E-Signature Infrastructure

The infrastructure required for the usage of e-signature

Information Security Infrastructure

Authentication, confidentiality, integrity and non-repudiation services for file, folder, and e-mail is provided by signature and encryption infrastructure

Principal based Management

Whole system is administrated according to the defined principals

Definite Hierarchy

Under the root certificate hierarchy, any number of vertical and horizontal certificate authorities can be defined. Also cross certificates can be issued to other certificate authorities.

Certificate Authority (CA) Components

Management Center (MC)

CAs and sub-CAs are administrated from Management Center by Administrators. Registrars, Administrators and Auditors can be created and authorized in MC.

Registration Authority(RA)

Registrars create and manage users/end entities, request certificates for them from CCS services, and personalize smartcards in RA.

Certificate Creation Service (CCS)

Listens Certificate Management Protocol (CMP) requests over http and generates certificates for the incoming requests to the CA.

Certificate Revocation Service (CRS)

Issues the Certificate Revocation List (CRL), for the certificates revoked for several reasons.

Online Certificate Status Protocol Service (OCSPS)

Certificate status can be queried online from OCSP Service.

Advantages

High Technology

- HSM and smartcard usage for high security
- Compliance to international security standards

Multi CA Creation/Management

- Any number of CA be created and managed via single interface

Ease of Usage and Integration

- All components of CA can easily be used and administrated from internet browser via user friendly modern interface
- Integration to CRM/ERP systems via web services
- Multi-Language support (Turkish/English/Azerbaijanese/Russian/Turkoman)

International Security Certificate

- Common Criteria EAL 4+ certificate compliant to Certificate Issuing And Management Components (CIMC) protection profile

Smartcard Printer Integration

- Integration with some smartcard printers for batch certificate personalization and easy integration infrastructure for new printers