ESYA
Electronic Signature Libraries
Technical Specifications

Supported Standards

- ETSI TS 101 733 CAdES e-signature format
- ETSI TS 101 903 XAdES e-signature format
- ETSI TS 102 918 Associated Signature Containers(ASiC)
- ETSI TS 102 204 Mobile Signature Service
- X.509 v3 Certificates
- X.509 v2 Certificate Revocation Lists (CRL)
- RFC 5280 Certificate Validation
- RFC 2560 Online Certificate Status Protocol (OCSP)
- RFC 3161 Timestamp Protocol
- LDAP Protocol

Basic Security Functions

- Symmetric and asymmetric cryptography functions
- Data encryption/signing using X.509 certificates
- Decryption/validation of encrypted/signed data using X.509 certificates and smartcards.

Cryptographic Features

- RSA and Elliptic Curve algorithms
- Use of SHA-1 and SHA-2 family of hash algorithms

Cryptographic Hardware Support

- PKCS 11 compliant smartcards and tokens
- APDU support for AKIS Smartcard OS
- Working with Hardware Security Module(HSM)

Proprietary Features

- All products are developed by TÜBİTAK BİLGEM UEKAE.
- Customization can be performed easily on request.
- National cryptographic algorithm support can be provided on request.

TÜBİTAK
BİLGEM

Electronic Certificate Management Infrastructure
Electronic Signature Libraries

Institutions/organizations, IT investments increase by the day passes, hardware and software parks grow like a snowball. One of the biggest challenges of this growing up is that every new hardware and product needs to be integrated with existing systems. While using products of information security, the integration needs more attention since ensuring the security of the systems requires lots of expertise. Hence, institutions/organizations generally prefer experts when they are seeking information security solutions.

ESYA e-signature libraries, developed with BİLGEM's more than ten years of e-signature experience, enable fast and secure electronic signing. Also they are fully compatible with international standards and they complete the security tests successfully. The libraries are implemented in JAVA and .NET platforms in order to provide easy and convenient integration with e-signature technology.

Features

Compatibility with Standards

- ETSI TS 101 733 CAdES electronic signature format (ASN data structure)
- ETSI TS 101 903 XAdES electronic signature format (XML data structure)
- ETSI TS 102 918 Associated Signature Containers

Supported Signature Types

- Basic Electronic Signature (ES-BES)
- Electronic Signature with Time (ES-T)
- Explicit Policy-based Electronic Signature (ES-EPES)
- ES with Complete Validation Data References (ES-C)
- Extended Electronic Signature with Time (ES-X)
- Extended Long Electronic Signature (ES-XL)
- Archival Electronic Signature (ES-A)

Supported Signature Features

- Signer's institution and authorization information
- Signing time at which signer claims
- Timestamp information which taken from secure timestamp server
- Signer location information like country, city and address
- Commitment type indication like proof of origin ,receipt, delivery ,sender
- MIME type of signed document can be added.

Supported actions on signed data

- Signed Document (Add/Remove)
- Signatures (Add/Remove)
- Certificates (Add/Remove)

Other Features

- Offline-online CRL and OCSP control for certificate validation
- NIST PKITS compatible certificate validation, bridge and cross- certification support
- Proprietary Certificate Store
- Multiple serial/parallel signature support

Advantages

Compatibility with Standards

- Fully compatible with national and international standards, laws, regulations and public acts.

Full Integration with Security Infrastructure

- Fully compatible with PKI standards
- Easy access to certificate and key services.

Customizable Signature Validation

- Certificate and Signature validation process is customizable via policy file and programming interfaces.

Mobile Technology

- Android device support
- Mobile signature support

Smart Card Support

- Compatibility with different smartcard and token brands
- High speed usage of AKIS smartcard with APDU