ESYA Elektronik İmza Kütüphaneleri Teknik Özellikleri

Desteklenen Standartlar

- ETSI TS 101 733 CAdES E-imza formatı
- ETSI TS 101 903 XAdES E-imza formatı
- ETSI TS 102 204 Mobile Signature Service
- ETSI TS 102 918 Associated Signature Containers (ASiC)
- X.509 v3 Sertifikalar
- X.509 v2 Sertifika İptal Listeleri (SİL/CRL)
- RFC 5280 Sertifika Doğrulama
- RFC 2560 Çevrimiçi Sertifika Durum Protokolü (ÇiSDuP/OCSP)
- RFC 3161 Zaman Damgası
- LDAP protokolü

Temel Güvenlik Hizmetleri

- Simetrik ve asimetrik kriptoloji fonksiyonları
- X.509 sertifikalarını ve açık anahtar algoritmalarını kullanarak imzalama ve imza doğrulama işlemleri

Sertifika ve Kripto Özellikleri

- RSA ve Eliptik Eğri algoritmaları ile hazırlanmış X.509 v3 sertifikalar ile çalışma
- SHA-1 ve SHA-2 ailesi mesaj özeti algoritmaları

Kripto Donanımı Desteği

- PKCS 11 uyumlu akıllı kartlarla ve çubuklarla çalışma
- AKIS kartlarla APDU yöntemi ile hızlı çalışma
- Donanımsal güvenlik modülleri (HSM) ile çalışma

Milli Özellikler

- Tüm yazılımlar TÜBİTAK BİLGEM UEKAE tarafından geliştirilmiştir.
- İsteğe bağlı olarak kısa sürede özelleştirme yapılabilir.
- İsteğe bağlı olarak milli kripto algoritması desteği verilebilir.

TÜBİTAK
BİLGEM

Elektronik Sertifika Yönetim Altyapısı

Elektronik İmza Kütüphaneleri

Kurum/kuruluşların bilişim yatırımları her geçen gün artmakta, donanım ve yazılım parkları çığ gibi büyümektedir. Bu büyümenin getirdiği en büyük sorunlardan biri alınan her yeni donanım ve sistemin mevcut sistemlerle entegre edilmesi zorunluluğudur. Bilgi güvenliği ile ilgili ürünlerin kullanımında, bu sorunun aşılması daha da zorlaşmaktadır. Çünkü sistemlerin güvenliğini sağlamak için yapılacak çalışmalar çok fazla uzmanlık gerektirmektedir. Bu nedenle kurum/kuruluşlar bilgi güvenliği sorunlarını aşarken genelde bu konunun uzmanı firmaların ürünlerini tercih etmektedir.

ESYA e-İmza kütüphaneleri, BİLGEM'in 10 yılı aşkın e-İmza deneyimiyle üretilmiş olup, güvenliği ve standartları belirlenmiş, kullanımı kolay ara yüzleriyle, imzalama işlemlerinin hızlı ve güvenli bir şekilde yapılmasına imkân verir. Yazılımlara kolayca e-İmza entegrasyonu yapılabilmesi için Java ve .NET platformlarında yazılım kütüphaneleri geliştirilmiştir.

Özellikler

Desteklenen Standartlar

- ETSI TS 101 733 CADES standardında elektronik imza formatı (ASN veri yapısı)
- ETSI TS 101 903 XADES standardında elektronik imza formatı (XML veri yapısı)
- ETSI TS 102 918 ASiC standardında elektronik imza formatı

Desteklenen İmza Tipleri

- Temel imza (ES-BES)
- Zaman damgalı imza (ES-T)
- İlke temelli imza (ES-EPES)
- Doğrulama referanslarıyla imza (ES-C)
- Referansları korumalı imza (ES-X)
- Uzun dönemli imza (ES-XL)
- Arşiv imzası (ES-A)

Desteklenen İmza Özellikleri

- İmza atan kişinin kurum ve yetki bilgileri
- Beyan edilen imza zamanı
- Güvenli zaman damgası sunucusundan alınmış zaman damgası bilgisi
- İmzanın atıldığı yer, ülke, şehir, adres bilgileri
- Belgeyi üreten, gönderen, teslim eden, alan, onaylayan gibi imza amacı bilgisi
- İmzalanan belgenin doküman formatı bilgisi eklenebilir.

İmza Yapısı Üzerinde Yapılabilecek İşlemler

- İmzalanan Belge (ekleme/çıkarma)
- İmzalar (ekleme/çıkarma)
- Sertifikalar (ekleme/çıkarma)

Diğer Özellikler

- Sertifika geçerlilik kontrolleri için, çevrimiçi-çevrimdışı SİL ve ÇiSDuP kontrolleri
- NIST PKITS uyumlu sertifika doğrulama, çapraz ve köprü sertifikasyon desteği
- Milli Güvenli Sertifika Deposu
- Bir belgeye birden çok seri/paralel imza ekleme

Sunulan Avantajlar

E-İmza Standartları

- Uluslarası ve ulusal e-İmza standart, kanun, tüzük ve yönetmeliklerine tam uyum

Güvenlik Altyapısı

- PKI standartlarına tam uyum
- Sertifika ve anahtar hizmetlerine zahmetsiz erişim

Esnek İmza Doğrulama Özelliği

- Sertifika ve imza doğrulama işlemlerinin, politika dosyaları ve arayüzlerle konfigüre edilebilme kabiliyeti

Mobil Teknoloji

- Android cihazlarda çalışabilirlik
- Mobil imza desteği

Akıllı Kart Desteği

- Farklı markaların akıllı çubuklarıyla işlem yapabilme
- APDU ile Akis akıllı kartlarda daha hızlı işlem yapabilme