MA3 API ELEKTRONİK İMZA KÜTÜPHANELERİ Teknik Özellikleri

Desteklenen Standartlar

- ETSI TS 101 733 CADES E-İmza formatı
- ETSI TS 101 903 XADES E-İmza formatı
- ETSI TS 102 778 PADES E-İmza formatı
- ETSI TS 102 918 ASIC E-İmza formatı
- ETSI TS 102 204 Mobil İmza Servisi
- 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-2 ailesi mesaj özeti algoritmaları

Kripto Donanımı Desteği

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

Milli Özellikler

- Yazılımlar TÜBİTAK BİLGEM tarafından geliştirilmiştir.

TÜBİTAK BİLGEM

AÇIK ANAHTAR ALTYAPISI KÜTÜPHANELERİ

MA3 API Elektronik İmza Kütüphaneleri

MA3 API E-İmza Yazılım kütüphaneleri, BİLGEM'in 20 yılı aşkın E-İmza deneyimiyle üretilmiş olup, güvenliği ve standartları belirlenmiş, kullanımı kolay arayüzleriyle, 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 İmza formatı (ASN veri yapısı)
- ETSI TS 101 903 XADES standardında Elektronik İmza formatı (XML veri yapısı)
- ETSI TS 102 778 PADES standardında Elektronik İmza formatı (PDF veri yapısı)
- ETSI TS 102 918 ASIC standardında Elektronik İmza formatı

Desteklenen İmza Tipleri

- Anlık imza (ES-BES)
- Zaman damgalı imza (ES-T)
- İlkeli imza (ES-EPES)
- 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 kart okuyucuları ile işlem yapabilme
- APDU ile AKİS akıllı kartlarda daha hızlı işlem yapabilme
- Donanım güvenlik modülleri (HSM) desteği