ESYA E-imza Kütüphaneleri

Ahmet Yetgin
Uzman Araştırmacı

Nisan 2012, İstanbul

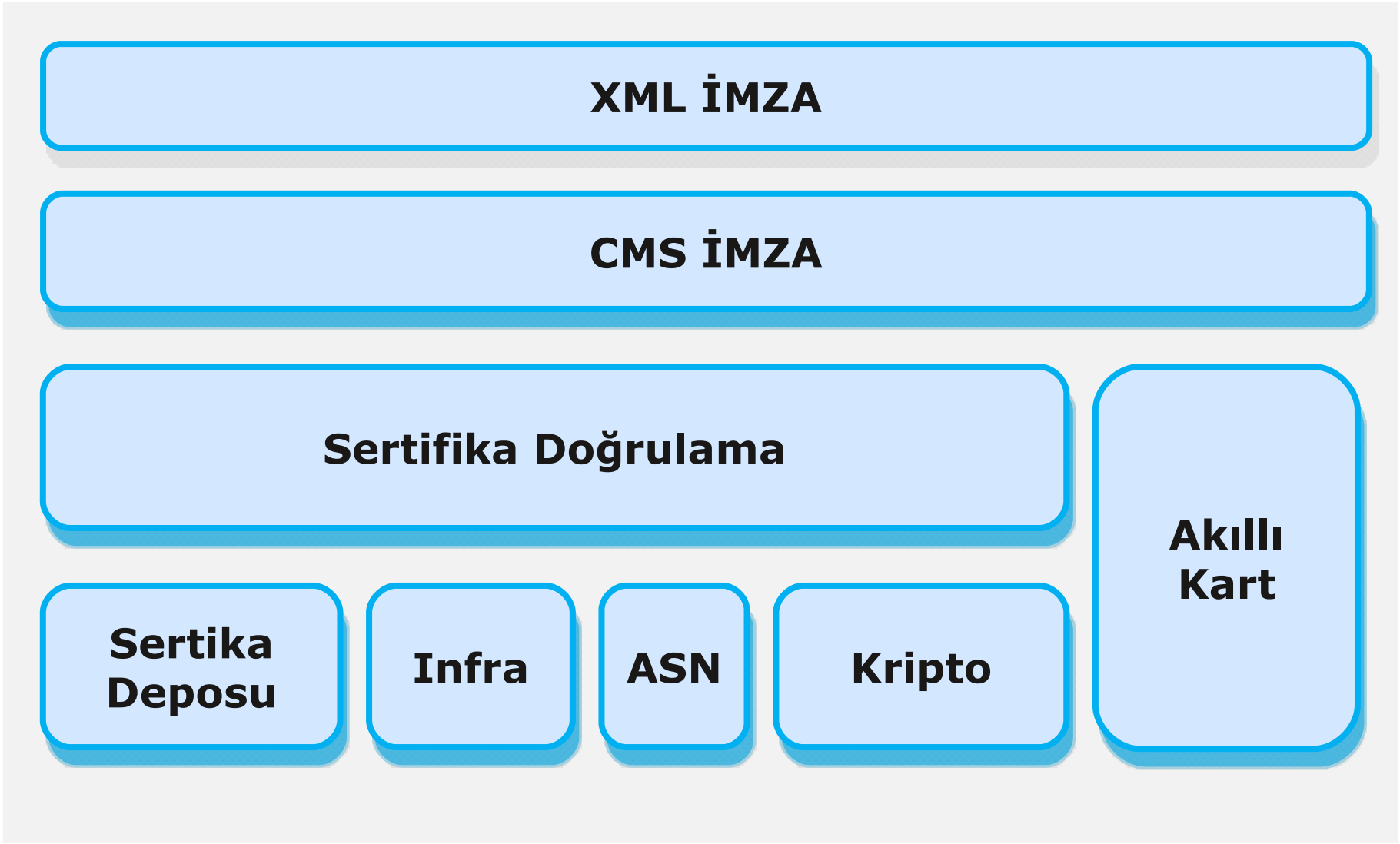
Gündem

- Neden ESYA API
- API Bileşenleri
- Sertifika Doğrulama
- Elektronik İmza

Neden ESYA API ?

- Standartlara uyumlu
- Milli
- Ama global
- Esnek / Konfigüratif

ESYA API Bileşenleri



Bileşenler - Kripto Kütüphanesi

- Modüler
- Gelişkin
  - SHA2
  - Elliptic Curve
  - RNG
    - Donanım modülü
    - Yazılımsal

Bileşenler - Kripto Kütüphanesi

İmzalama

- Signer (BaseSigner)

Şifreleme

- Cipher (BaseCipher)

Bileşenler – ASN Kütüphanesi

Abstract Syntax Notation One (ASN.1)

Anahtar sınıflar

- ECertificate
- ECRL
- EOCSPResponse

Bileşenler – Infra(structure) Kütüphanesi

Kaynaklara erişim

- Dizin
- ÇiSDuP (OCSP)
- Zaman damgası

Bileşenler - Akıllı Kart Kütüphanesi

Kriptografik işlemler için güvenli ortam

Kullanım örnekleri

- Sertifika Okumak
- Şifreleme/imzalama
- PKCS7 / BES imza

Bileşenler - Akıllı Kart Kütüphanesi

- Java 6 ile ekstra
  - Java 6 kart tipi tanıma desteği
  - Java 6 AKIS APDU(application protocol data unit) desteği
- Java Akıllı Kart API'si küçük uygulamalar için optimize
  - smartcard ve common .jar yeterli

Bileşenler - Sertifika Deposu

Sertika Deposu

- Doğrulama kaynaklarına yerel erişim
- Güvenilir sertifikalar, SİL vb.

- İmza doğrulama için gerekli.

- Güvenli!

  Kanuni olarak güvenilir sertifikalar KamuSM tarafından imzalı.

Bileşenler - Sertifika Doğrulama Kütüphanesi

- Standartlara uygun
  - X.509 Açık Anahtar Altyapısı (Sertifika, SİL vb.)
  - RFC 4158 - Zincir oluşturma
  - RFC 5280 - Yapısal ve Zincir doğrulama
- Konfigüratif
  - Sertifika doğrulama konfigurasyonu
  - Sertifika deposu

Sertifika Doğrulama

Bileşenler

- Bulucu
- Eşleştirici
- Kontrolcü

Sertifika Doğrulama

Kontrolcüler

Sertifika ve SİL'lerin

- Yapısal özelliklerinin
- Sertifika zincir ilişkisinin

standartlara uygunluğunu kontrol eden sınıflardır.

Sertifika Doğrulama

Bulucular (Finder)

- Güvenilir Sertifika
- Sertifika
- Doğrulama Verisi
  - SİL
  - ÇİSDuP

Nereden?

- Sertifika Deposu
- Online kaynaklar HTTP/LDAP
- Dosya Sistemi

Sertifika Doğrulama

Eşleştiriciler (Matcher)

- Bulunan doğrulama verisi (Sertifika, SİL, OCSP cevabı) aranılan veriler mi?
  - RFC 5280

Sertifika Doğrulama

Kaydediciler (Saver)

- Bulunan kaynakların tekrar kullanımı

Sertifika Doğrulama

- XML Tabanlı Konfigürasyon

```
<policy>
    <find> ... </find>
    <match> ... </match>
    <validate> ... <validate>
<policy>
```

Sertifika Doğrulama

```
ValidationPolicy policy = PolicyReader.readValidationPolicy(
            new FileInputStream(POLICY_FILE));

ValidationSystem vs =
            CertificateValidation.createValidationSystem(policy);

vs.setBaseValidationTime(Calendar.getInstance());

CertificateStatusInfo csi =
            CertificateValidation.validateCertificate(vs, cert);
```

Elektronik İmza

3 ana özellik :

- Kimlik doğrulama ve onaylama,
- Veri bütünlüğü
- İnkar edilememezlik

Elektronik İmza

- CAdES

  ASN.1 yapı

  - RFC 3852 (CMS)
  - ETSI TS 101 733 – v1.8.1

- XAdES

  XML yapı

  - W3C XMLdSig
  - ETSI TS 101 903 - v1.4.2

İmza Tipleri

- **ES-BES**
- ES-EPES
- **ES-T**
- ES-C
- ES-X Type 1-2
- **ES-X-Long**
- ES-A(rchive)

İmza Profilleri

- Anlık
- Kısa Ömürlü
- Uzun Ömürlü
  - SİL
  - OCSP

https://yazilim.kamusm.gov.tr

- Test sertifikası
- Test lisansı
- API bundle
- Test zaman damgası

İmza atma

```
BaseSignedData bs = new BaseSignedData();
bs.addContent(new SignableByteArray("test".getBytes()));

Map<String, Object> params = ...; // setup

ValidationPolicy policy=  ...; // read

ECertificate cert = new ECertificate(new File(SIGNING_CERTIFICATE_PATH));

SmartCard sc = … ; // init

BaseSigner signer = new SCSignerWithCertSerialNo (sc, session, slot,

cert.getSerialNumber().toByteArray(), SignatureAlg.RSA_SHA256.getName());


/*add signer. Since the specified attributes are mandatory for bes,null is
given as parameter for optional attributes*/

bs.addSigner(ESignatureType.TYPE_BES, cert , signer, null, params);

AsnIO.dosyayaz(bs.getEncoded(),SIGNATURE_FILE);
```

Akıllı Kart Kullanımı

- XAdES

```
BaseSigner signer = getSmardCardSigner();
signature.sign(signer);
```

Ayrık İmza

İmzalanan veri büyük olduğunda ayrık imza kullanılmalı

- CAdES

```
baseSigneddata.addContent(signable,false);
```

- XAdES

```
signature.addDocument(fileName, mimeType, false);
```

Çoklu imzalar

- Paralel İmza
  - İmzalar aynı seviyede
  - Bir imza çıkarsa...
- Seri İmza (Counter Signature)
  - İmzayı imzalama
  - Bir imza çıkarsa, serideki sonraki imzalar da çıkarılmalı...

Çoklu imzalar

- **CAdES Paralel İmza**

```
byte[] signatureBytes = AsnIO.dosyadanOKU(SIGNATURE_FILE);
BaseSignedData bsd = new BaseSignedData(signatureBytes);
…
bsd.addSigner(...);
```

- **CAdES Seri İmza;**

```
BaseSignedData bs = new BaseSignedData(signatureBytes);
…
Signer firstSigner = bs.getSignerList().get(0);
firstSigner.addCounterSigner(ESignatureType.TYPE_BES, cert ,
signer, null, params);
```

Çoklu İmzalar - XAdES

- SignedDocument

```
<?xml version="1.0" encoding="UTF-8" ?>
<ma3:envelope ...>

    <ma3:data>
        <ma3:data-item>...</ma3:data-item>
        <ma3:data-item>...</ma3:data-item>
        …
    <ma3:data>

    <ma3:signatures>
        <ds:signature>...</ds:signature>
        <ds:signature>...</ds:signature>
        ...
    </ma3:signatures>

</ma3:envelope>
```

İmza Tipleri Arası Dönüşüm

- CAdES

```
signedData.getSignerList().get(0)
          .convert(ESignatureType.TYPE_EST, params);
```

- XAdES

```
signature.upgradeToXAdES_T();
```

İmza Doğrulama

- CAdES

```
params.put(EParameters.P_EXTERNAL_CONTENT, content );

SignedDataValidation sdv = new SignedDataValidation();

SignedDataValidationResult sdvr = sdv.verify(signedData,
params);
```

- XAdES

```
ValidationResult result = signature.verify();
```

Arşiv Tipi Elektronik İmza

- Arşiv tipine çevrim
  - Kriptografik metodların zaman içinde zayıflaması
  - Son zaman damgasını imzalayan sertifikanın ömrünün sonuna yaklaşması

Sorular