TÜBİTAK BİLGEM

XAdES XML E-İmza Formatı

ve ESYA Yazılım Kütüphaneleri

Ahmet Yetgin
ahmet.yetgin@tubitak.gov.tr

Kasım 2012

Ajanda

Kavramlar

XML İmza (XMLdSig)

XAdES

ESYA API

Kavramlar - Kriptografi

Kriptografi,

Haberleşen iki veya daha fazla tarafın bilgi alışverişini

emniyetli bir şekilde yapmasını sağlayan,

temeli matematiksel zor problemlere dayanan teknik ve uygulamaların bütünüdür.

Kavramlar - Haberleşmede Güvenlik Ögeleri

- Gizlilik (Confidentiality of Content)
- Bütünlük (Integrity of Content)
- Kimlik Doğrulaması (Authentication of Origin)
- İnkar Edememezlik (Non-repudiation)
- Süreklilik

Krtiptografik Teknikler

- Simetrik Kriptografi
  - Gizli anahtar (Secret Key)
- Asimetrik Kriptografi
  - Özel anahtar (Private key) Açık anahtar (Public Key)
- Özet fonksiyonu
  - Sabit boy, küçük değişikliklere duyarlı, tek yönlü, hızlı
- Sayısal imza
  - İnkar edememezlik, Asimetrik kriptografi

E-İmza Nedir

5070 sayılı Kanun'daki tanım:

"*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*"

Elektronik ortamda

- Bir metni onaylama
- Bir anlaşmayı veya sözleşmeyi kabul etme

3 ana özellik :

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

Kavramlar - XML

eXtensible Markup Language

W3C tavsiyesi, 10 Şubat 1998
http://www.w3.org/TR/REC-xml

Veri taşıma ve saklama

XML
- tag
- attribute
- namespace

Örnek XML

```
<?xml version="1.0" encoding="UTF-8" ?>
<envelope xmlns="http://tubitak.gov.tr/xml/signature#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

    <data>
        <data-item Id=”data-1”>Örnek veri</data-item>
        <data-item Id=”data-2”>...</data-item>
        ...
    <data>

    <signatures>
        <ds:signature>...</ds:signature>
        ...
    </signatures>
</envelope>
```

XML İmza

XMLdSig

IETF/W3C Tavsiyesi

http://www.w3.org/TR/xmldsig-core/

1. sürüm 2002
2. sürüm Haziran 2008, Ver 1.1

İmzalanan Veriye Referans

XML İmza, bir ya da daha fazla referans ile gösterilen veri ve bir anahtar arasında ilişki kurmaktır.

XMLdSig bir anahtarın kişi yada kurumla nasıl ilişkilendirildiği ile ilgilenmez.

XML İmza

XML Dökümanın sadece bir kısmını imzalamak için kullanılabilir. Dökümanın farklı bölgelerinde farklı imzalar olabilir.

İmzalanan veri XML formatında olabilir/olmayabilir

İmzalanan Veriye Referans

XML İmza bir URI ile veriye bağlı olabilir

- Ayrık imza (detached)

İmza, imzalanan veri ile aynı seviyede olabilir.

- Zarflanmış imza (enveloped)

İmza, imzalanan verinin içinde yer alabilir.

- Zarflanmış imza (enveloped)

İmzalanan veri, imzanın içinde yer alabilir

- Zarflayan imza (enveloping)

İmzalanan Veriye Referans

İmzalanan her bir veri

<Reference> elemanı ile tanımlanır

Tipik bir **<Reference>** elemanı

- imzalanan veriye işaret eder - **URI**
- bir özet metodu belirler (örneğin SHA-256)
- imzalanacak verinin özetini
  base 64 notasyonunda barındırır

<Reference> Elemanı

```
<Reference URI = “http://.../po.xml”>
    <Tranforms...
    <DigestMethod Algorithm=”Örneğin SHA-256”/>
    <DigestValue>po.xml’e ait özet değeri
    </DigestValue>
</Reference>
```

Transformasyonlar

Canonicalization

XML metin sunumunu tekilleştirme

Base64

Binary veriyi metin formatında kullanmak

XSLT

XML kaynağı üzerinde tam XSLT dönüşümü

XPath

İmza için bir dökümanın parçalarını filtrelemek

İmzalanan Veriye Referans

İmzada birden fazla referans olabilir

<Reference>
URI, özet metodu, özet değeri
</Reference>
:
<Reference>
URI, özet metodu, özet değeri
</Reference>

İmzalanan Alan

Referanslar SignedInfo içindedir

<SignedInfo>
<CanonicalizationMethod>SignedInfo'ya uygulanacak algoritma
<SignatureMethod>Örneğin RSA-Sha256

<Reference ...
<Reference ...
</SignedInfo>

İmza Değeri

İmza değeri hesaplanır

<SignedInfo>
    <CanonicalizationMethod>SignedInfo'ya uygulanacak algoritma

    <SignatureMethod>Örneğin RSA-Sha256

    <Reference ...
    <Reference ...
</SignedInfo>

<SignatureValue>Base 64 imza değeri
</SignatureValue>

İmzacı Sertifikası

Sertifika eklenir

<SignedInfo..
<SignatureValue..
<KeyInfo>
<X509Data>
<X509Certificate>Base64 formatında, bir SM tarafından imzalanmış açık anahtar ve kimlik bilgisi -
</X509Certificate>
</X509Data>
</KeyInfo>

Bütün Halde İmza

Signature elemanı içinde

```
<Signature>
    <SignedInfo>
        ...
        <Reference
        <Reference
    </SignedInfo>

    <SignatureValue>Base 64 imza değeri</SignatureValue>

    <KeyInfo>...
    <Object>...
</Signature>
```

Güvenlik

- SM imzalı sertifika değiştirilip başkası imza atmış gibi gösterilebilir mi?
- Referans URI değiştirilebilir mi?
- Canonicalization method değiştirilebilir mi? İmza metodu değiştirilebilir mi?

Doğrulama

- İmza Doğrulama
  - SignedInfo C14n
  - Özetini al
  - Açık anahtarı bu değerle işlemden geçirip,
    - SignatureValue uygun mu kontrol et
- Referans doğrulama
  - Referanslardaki verilerin özetini kontrol et
- Sertifika doğrulama

Yapısına Göre İmzalar

Zarflayan (Enveloping) imza

Veri imzanın içinde

```
<Signature
   <SignedInfo …
      <Reference URI=”#data-1”...
      ...
   <KeyInfo ...
   <Object Id=”data-1”>
      <ereceteBilgisi>...</ereceteBilgisi>
   </Object>
</Signature>
```

Yapısına Göre İmzalar

Ayrık (Detached) İmza

```
<Signature
    <SignedInfo …
        <Reference URI=”recete.xml”...
        ...
    <KeyInfo ...
</Signature>
```

Dosya: recete.xml

```
<ereceteBilgisi>...</ereceteBilgisi>
```

Yapısına Göre İmzalar

Zarflanmış imza:

```
<ereceteBilgisi>
...
    <Signature
        <SignedInfo …
            <Reference URI=””>
                <Transforms>
                    <Transform Algorithm=
                                "...#enveloped-signature"/>
                ...
        <KeyInfo ...
    </Signature>
</ereceteBilgisi>
```

XAdES

Avrupa Birliği Direktifi 1999/93/EC

XAdES (XML Advanced Signature)

http://uri.etsi.org/01903/v1.4.1/

v1.1.1 2002
v1.4.1 15.6.2009

XAdES

```
<Signature>
    <SignedInfo>...
    <SignatureValue>Base 64 imza değeri</SignatureValue>
    <KeyInfo>...

    <Object>
            <QualifyingProperties>
                <SignedProperties ...
                <UnsignedProperties ...
            </QualifyingProperties>
    </Object>
</Signature>
```

XAdES

```
<Signature>
    <SignedInfo>
        ...
        <Reference URI=”#signedprops-1”...
    </SignedInfo>
    ...
    <Object>
        <QualifyingProperties>
            <SignedProperties Id=”signedprops-1”...
            <UnsignedProperties ...
        </QualifyingProperties>
    </Object>
</Signature>
```

BES (Basit Elektronik İmza)

Sertifika bilgisi imza değeri içine alınır:

```
<QualifyingProperties>
   <SignedProperties>
      <SignedSignatureProperties>
         <SigningTime>
         <SigningCertificate ...
         ...
      <SignedDataObjectProperties>
         <DataObjectFormat ...
```

BES (Basit Elektronik İmza)

```
<SigningCertificate>
<Cert>
    <CertDigest>
        <ds:DigestMethod Algorithm="...#sha256"/>
        <ds:DigestValue>k6vd5m...=</ds:DigestValue>
    </CertDigest>
    <IssuerSerial>
        <ds:X509IssuerName>CN=Kamu Elektronik Sertifika
                Hizmet Sağlayıcısı ...</ds:X509IssuerName>
        <ds:X509SerialNumber>70..</ds:X509SerialNumber>
    </IssuerSerial>
</Cert>
</SigningCertificate>
```

EPES (Politika Temelli İmza)

Politika bilgisi imzaya eklenir:

```
<QualifyingProperties>
   <SignedProperties>
      <SignedSignatureProperties>
         <SigningTime>
         <SigningCertificate>
         <SignaturePolicyIdentifier...
         ...
      <SignedDataObjectProperties>
         <DataObjectFormat>
```

ES-T (Zaman Damgalı İmza)

Zaman damgası

```
<QualifyingProperties>
   <SignedProperties>
      ...
   <UnsignedProperties>
      <UnsignedSignatureProperties>
         ..
         <SignatureTimeStamp …
      ...
   </UnsignedProperties>
```

Doğrulama Verisi ve İmza

<UnsignedSignatureProperties

<CompleteCertificateRefs>
<CompleteRevocationRefs>
...

ES-C

<SigAndRefsTimeStamp>
| <RefsOnlyTimeStamp>

ES-X

<CertificatesValues>
<RevocationValues>
...

ES-XL

Arşiv Formatı

- Elektronik imzalı dokümanların uzun dönem saklanması gerektiğinde
- Geçmişte kullanılan algoritmaların veya anahtarların artık güvenli kabul edilmediği durumlarda
- Son zaman damgasını imzalayan sertifikanın ömrü dolmadan

<UnsignedSignatureProperties

...

<xadesv141:ArchiveTimeStamp

<xadesv141:TimeStampValidationData

İmza Tipleri

İmza Tipi	Özellik
ES-BES	Basit
ES-EPES	Politika temelli
ES-T	Zaman damgalı
ES-C	Doğrulama verisine referans
ES-X Type1- Type2	Referanslar korumalı
ES-XL	Doğrulama verisi ekli
ES-A	Arşiv

İmza Profilleri

http://www.tk.gov.tr/bilgi_teknolojileri/elektronik_imza/dosyalar/Elektronik_Imza_Kullanim_Profilleri_Rehberi.pdf

Profil	İmza Ömrü	Zaman Damgası	İmza Formatı	Kesinleş-me Süresi	İptal Bilgisi	Dosya boyutu
P1	Anlık	-	ES-Bes	-	SİL / ÇiSDuP	Düşük
P2	Kısa	Var	ES-T	-	SİL	Orta
P3	Uzun Süreli	Var	ES-XL	Evet	SİL	Çok yüksek
P4		Var	ES-XL	-	ÇiSDuP	Yüksek

Ayrık İmza Yaklaşık Uzunlukları

Eİmza Tipi	**Profil**	**CAdES**	**XAdES**
ES-BES	P1	3 KB	5 KB
ES-T	P2	6 KB	11 KB
ES-XL	P3 (SİL)	20 KB	45 KB
ES-XL	P4 (OCSP)	15 KB	37 KB
AS-A	P4+Arşiv	25 KB	43 KB

Çoklu İmzalar

- Paralel imza
  - İmzalar aynı seviyede
  - Birbirinden bağımsız...

- Seri imza (Counter signature)
  - İmzayı imzalama
  - Bir imza çıkarsa, serideki sonraki imzalar da çıkarılmalı...

Çoklu İmzalar

- Seri İmza

```
<Signature>
    ...
    <UnsignedSignatureProperties>
      <CounterSignature> *
```

- Paralel İmza

```
<Signature>..</Signature>
<Signature>..</Signature>
```

Çoklu İmzalar

SignedDocument sınıfı çoklu imzalar için kullanılır:

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

ESYA Kütüphaneleri

ESYA Yazılım Kütüphaneleri

http://yazilim.kamusm.gov.tr

ESYA Kütüphane Bileşenleri

ŞİFRELEME (CMS Envelope)

XML İMZA

CMS İMZA

Sertifika Doğrulama

Akıllı Kart

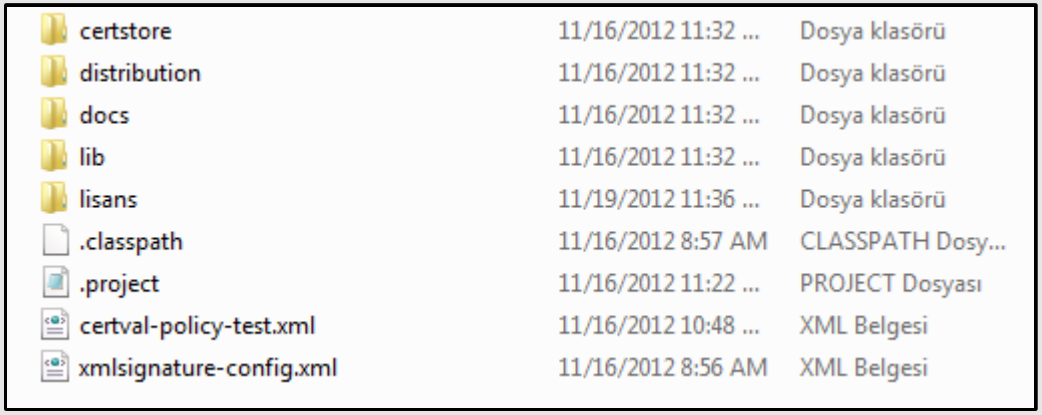
Sertika Deposu

Infra

AS N

Kripto

MA3-API XMLSignature 1.4.8.zip



certstore	11/16/2012 11:32 ...	Dosya klasörü
distribution	11/16/2012 11:32 ...	Dosya klasörü
docs	11/16/2012 11:32 ...	Dosya klasörü
lib	11/16/2012 11:32 ...	Dosya klasörü
lisans	11/19/2012 11:36 ...	Dosya klasörü
.classpath	11/16/2012 8:57 AM	CLASSPATH Dosy...
.project	11/16/2012 11:22 ...	PROJECT Dosyası
certval-policy-test.xml	11/16/2012 10:48 ...	XML Belgesi
xmlsignature-config.xml	11/16/2012 8:56 AM	XML Belgesi

XML İmza Konfigürasyon Dosyası

```
<?xml version="1.0" encoding="UTF-8"?>
<xml-signature-config ...>

    <locale language="tr" country="TR"/>
    <http>...
          …
     <timestamp-server>
        <host>http://tzd.kamusm.gov.tr</host>
        <digest-alg>SHA-1</digest-alg>
        <userid>number</userid>
        <password>top_secret</password>
    </timestamp-server>
      …
    <validation>
        <certificate-validation-policy-file>certval-policy-
test.xml</certificate-validation-policy-file>
...
```

Sertifika Doğrulama

```
// JSmartCardManager.java ile sertifika seç...

// Oturum bazlı sertifika doğrula
ValidationSystem vs = CertificateValidation
                    .createValidationSystem(getPolicy());
vs.setBaseValidationTime(Calendar.getInstance());
CertificateStatusInfo csi =
    CertificateValidation.validateCertificate(vs, cert);

// Aynı oturumda tekrar sertifika doğrulanmayabilir
Context context = new Context(BASE_DIR);
context.setValidateCertificates(false);
```

XAdES BES İmza Atma

```
Context context = new Context(BASE_DIR);

// context'e göre imza yarat
XMLSignature signature = new XMLSignature(context);

// dökümanı imzaya ekle
signature.addDocument("./sample.txt", "text/plain", true);

// add certificate to show who signed the document
signature.addKeyInfo(CERTIFICATE);

// kartla imzala
signature.sign(getCardSigner());

signature.write(new
FileOutputStream(SIGNATURE_FILENAME));
```

P2 İmza Atma

```
// context'e göre imza yarat
XMLSignature signature = new XMLSignature(context);

signature.setPolicyIdentifier(OID_POLICY_P2,
            "Kısa Dönemli ve SİL Kontrollü Güvenli Elektronik
İmza Politikası",            "
http://www.tk.gov.tr/bilgi_teknolojileri/elektronik_imza/dosyalar/
");

…

// kartla imzala
signature.sign(getCardSigner());

signature.upgradeToXAdES_T();
```

P3- P4 İmza Atma

```
...
signature.setPolicyIdentifier(OID_POLICY_Pn, ...

// kartla imzala
signature.sign(getCardSigner());

// zaman damgası ekle
signature.upgradeToXAdES_T();

// gerekiyorsa bekle
signature.upgradeToXAdES_C();
signature.upgradeToXAdES_X1();
signature.upgradeToXAdES_XL();
```

İmza Doğrulama

```
// İmzayı dosyadan oku
XMLSignature signature =
    XMLSignature.parse(new FileDocument(file),
                       new Context(BASE_DIR)) ;

// Doğrula
ValidationResult result = signature.verify();

// Detaylı doğrulama mesajı
System.out.println(result.toXml());

// Sonuç tipi
Assert.assertTrue("Cant verify " + fileName,
          result.getType() == ValidationResultType.VALID);
```

Neden ESYA Kütüphaneleri

- Standartlara uyumlu
  - E-İmza
    - ETSI Plugtestlerine 3 kez katılım
  - Sertifika Doğrulama
    - NIST Testleri %100 uyumluluk

Neden ESYA Kütüphaneleri

- Standartları belirliyoruz!
  - ETSI–ESI grubu faaliyetlerinde standartların belirlenmesine katılım
  - Türkiye'de kullanılan Sertifika / SİL /OCSP profillerinin oluşturulması
  - Türkiye'de kullanılacak E-İmza profillerinin oluşturulması ve BTK'ya yayınlanmak üzere iletilmesi
  - DPT nezdinde yürütülen E-Yazışma formatının belirlenmesine katılım (Pilot için kütüphane temini)

Neden ESYA Kütüphaneleri

Bilgi, alanında hakimiyet

- Destek
  - Kurumlara E-İmza süreçlerinin anlatılması,
- Denetim
  - 2007 yılından itibaren 47 kamu kurumu ve 5 özel kurumun e-imza uygulamaları incelenmesi
- E-İmza Uyumluluk Testleri

Sorular