TÜBİTAK BİLGEM

Açık Anahtar Altyapısı ve Eİmza
ESYA Yazılım Kütüphaneleri

Ahmet Yetgin
ahmet.yetgin@tubitak.gov.tr

Ocak 2013

Ajanda

Kriptografi ve AAA

API Bileşenleri

Akıllı kart

Sertifika Deposu

Sertifika Doğrulama

Eimza Nedir?

- Formatlar, Tipler,
- Türkiyede İmza Profilleri
- Çoklu İmza
- Arşivleme

Soru cevap

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

Kriptografik 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

Sertifika

- Sertifika sahibi hakkında bilgileri barındırırlar.
  - Adı – Soyadı, TC Kimlik Nosu, E-Mail adresi
  - Açık anahtarı
- Kullanıma giriş ve bitiş tarihi vardır.
- Güvenilir bir kurum tarafından yayınlanır.
  - Bu kurum tarafından imzalanmıştır.
- Yayıncı kuruluş (Issuer) ve seri numarası (serial number) bir sertifikayı tekil yapar.
  - SubjectKeyIdentifier'da tekildir. (Zorunlu alan değil)
- ECertificate

Örnek Sertifika

Seri No	2368
Sertifika Sahibi	Bora Uzun
Şirket/Kurum	Tübitak
Yayınlayan	KamuSM
E-posta Adresi	bora@tubitak.gov.tr
Yayın Tarihi	05.02.2012
Son Kullanım	05.02.2015
Açık Anahtar	2489349e894859f45489450dab4545 4ca0908d8809

KamuSM Sayısal İmzası	ae89349c989893e8989548d0823 048b08023f9e903

Sertifika İptal Bilgisi

Kullanıcı akıllı kartını çaldırdığı veya kaybettiği zaman sertifikasının iptal edilmesini isteyebilir.

İptal bilgisini öğrenmek için Sil ve OCSP hizmetleri kullanılır.

SİL – Sertifika İptal Listesi

Artık güvenilemeyecek olan ve kullanım süresi dolmamış sertifikaların seri numaralarını içerir.

Yayınlandığı tarihi ve son kullanım tarihini içerir.

Sertifikayı imzalayan kurum tarafından yayınlanır.

Yayınlayan kuruluşun adını ve sayısal imzasını içerir.

Sık aralıklarla yayınlanır.

Örnek SİL

Yayınlayan	**KamuSM**
Yayın Tarihi	**22.08.2007**
Son Kullanım	**24.08.2007**

İptal Olan Sertifikaların Listesi
55, 678, 2164, 3403, 4034, 5677 ....

UEKAE Sayısal İmzası	6656e345200cde989228d0823aec8b08023f9

Çevrimiçi Sertifika Durum Protokolü

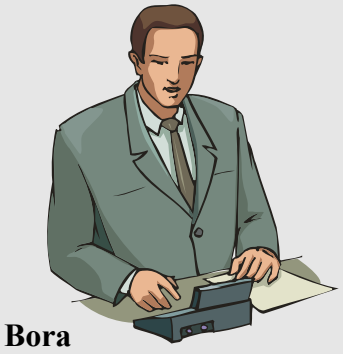
Kullanıcı isteği: X no'lu sertifikanın durumu nedir?

OCSP sunucusu yanıtı:

- İptal edilmemiş
- İptal edilmiş
  - İptal nedeni
  - İptal zamanı
- Bilinmiyor

E-imzalı Mesaj Oluşturma

Bora, Ayşe'ye Elektronik İmzalı Bir Mesajı Nasıl Gönderir?



Açık Mesaj

Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Özetleme Algoritması

Mesaj Özeti

Güvenli Elektronik İmza Aracı

Özel Anahtar

Bora

İmzalama Algoritması

Elektronik İmza

Gönderilen Paket

Açık Mesaj

Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Elektronik İmza

Elektronik Sertifika

·Tasnif Dışı

E-imzalı Mesaj Doğrulama

Ayşe, Bora'dan Gelen Elektronik İmzalı Bir Mesajı Nasıl Doğrular?

Bora
Elektronik Sertifika

Alınan Paket

Açık Mesaj
Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Elektronik İmza

Elektronik Sertifika

Açık Mesaj
Ankara'daki 12204 no'lu hesabıma 1,000 TL gönder

Özetleme Algoritması

Sertifika Kontrolleri (SİL – OCSP)

Elektronik İmza

Mesaj Özeti

=?

Açık Anahtar
Bora

Onaylama Algoritması

Onaylanmış Mesaj Özeti

ESYA Kütüphane Bileşenleri

ŞİFRELEME (CMS Envelope)

XML İMZA

CMS İMZA

Sertifika Doğrulama

Akıllı Kart

Sertika Deposu

Infra

ASN

Kripto

Akıllı Kart Kütüphanesi

- Kriptografik işlemler için güvenli ortam
- Kullanım örnekleri
  - Sertifika Okumak
  - Şifreleme/imzalama
  - PKCS7 / BES imza
- Java 6 ile kart tipi tanıma, AKİS APDU
- Küçük uygulamalar için optimize
  - smartcard ve common.jar yeterli

Sertifika Deposu

- Kütüphane ve Veritabanı
- Yerel Sertika Deposu
  - Doğrulama kaynaklarına yerel erişim
  - Güvenilir sertifikalar, SİL vb.
- XML Sertifika Deposu
  - Cache yok

  - İmza doğrulama için gerekli.
  - Güvenli!

  Kanuni olarak “güvenilir sertifikalar” KamuSM tarafından imzalı.

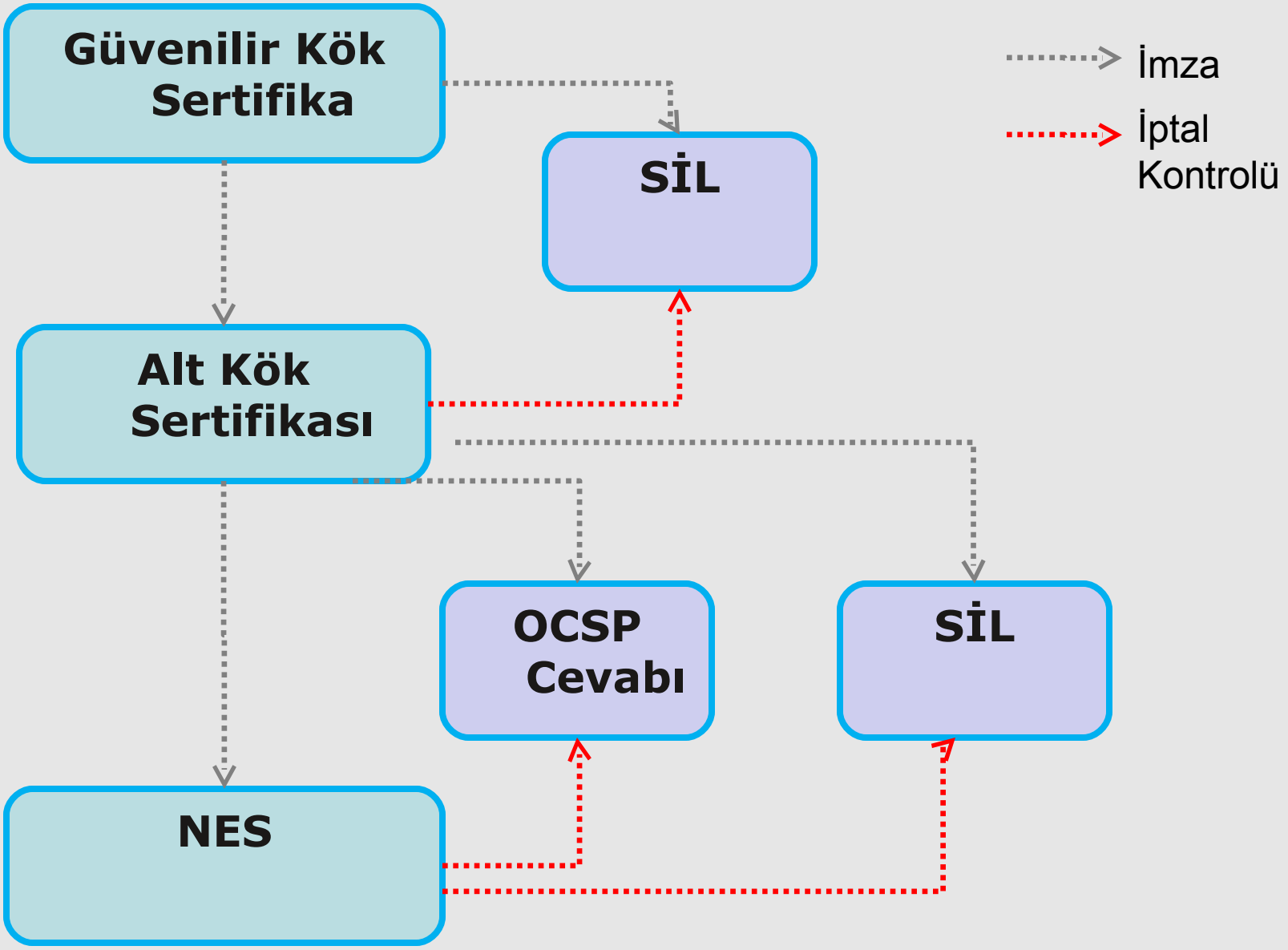
Sertifika Doğrulama

- Standartlara uygun
  - X.509 Açık Anahtar Altyapısı

    (Sertifika, SİL vb.)
  - RFC 4158 - Zincir oluşturma
  - RFC 5280 - Yapısal ve Zincir doğrulama
- Konfigüratif
  - XML tabanlı “Sertifika Doğrulama Konfigurasyonu”

    Bulucu, Eşleştirici, Kontrolcü, Kaydedici...
  - Sertifika deposu

Sertifika Doğrulama



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

İmza Formatları

1999: Elektronik imzalar için bir ortak çerçeve hazırlanması konusunda Avrupa Birliği Komisyonu direktifi

Format	Standart
CAdES (CMS Advanced Signature)	ETSI TS 101 733 V1.8.1 RFC 3852: Cryptographic Message Syntax (CMS)
XAdES (XML Advanced Signature)	ETSI TS 101 903 V1.4.2 W3C/IETF Recommendation: "XML-Signature Syntax and Processing".
PAdES (PDF Advanced Signature)	ETSI TS 102 778-3 V1.2.1, ETSI TS 102 778-4 V1.1.2, ETSI TS 102 778-5 V1.1.2
ASiC (Associated Signature Containers)	TODO

ESYA Gelişmiş İmza Kütüphaneleri

	JAVA	.NET
XAdES	+	+
CAdES	+	+
PAdES	-	-
ASiC	2012 içinde	2012 içinde

Yapısına göre imzalar

- Zarflı (Enveloping)
  - Veri imzanın içinde
- Ayrık (Detached)
  - İmza ve veri ayrı
- Zarflanmış (Enveloped / XAdES)
  - İmza verinin içinde

Çoklu İmzalar

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

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

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

Arşiv İmza

Elektronik imzalı dokümanların uzun dönem saklanması gerektiğinde

- Geçmişte kullanılan algoritmaların veya anahtarların artık güvenli kabul edilmediği durumlarda
- Son zaman damgasını imzalayan sertifikanın ömrü dolmadan

Sorular