TÜBİTAK
BİLGEM

Sertifika Doğrulama

Dindar ÖZ
Kermen Takım Lideri

Kasım 2012

Sunum Planı

- Giriş
- X.509 Sertifika Doğrulama
  - Zincir Oluşturma
  - Zincir Doğrulama
- ESYA API Sertifika Doğrulama Modülleri
- Demo
  - Örnek Kod ve Uygulama

Giriş

Temel Kavramlar

- Sertifikalar
- X.509
- Kök Sertifika Makamı(KSM)
- Sertifika Makamı (SM)
- ESHS
- Sertifika Zinciri
- SİL
- OCSP

5070 Sayılı Kanun

Madde 4 - Güvenli elektronik imza;

a) Münhasıran imza sahibine bağlı olan,

b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c) **Nitelikli elektronik sertifikaya** dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan,

Elektronik imzadır.

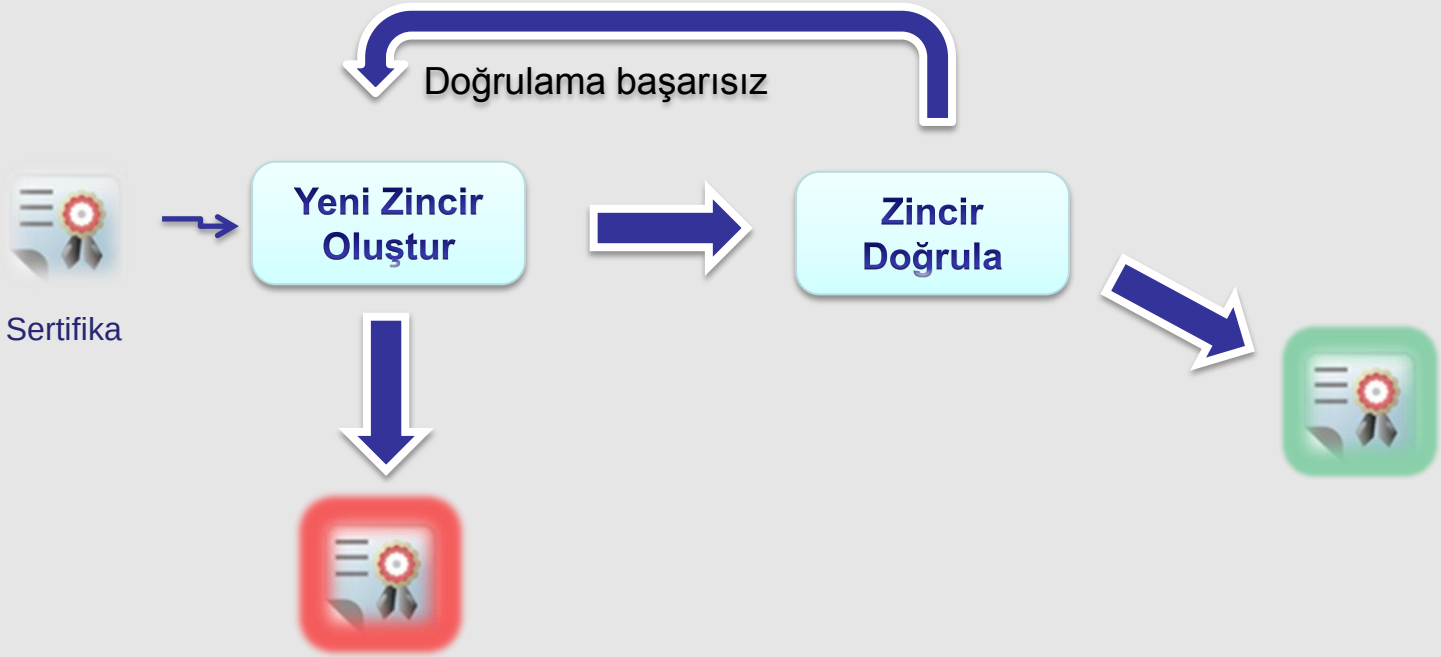
Sertifika Doğrulama

- Sertifikaların Sertifika Profilinde tanımlı Nitelikli Elektronik Sertifika standartlarına **biçimsel**, **mantıksal** ve **güvenlik** özellikleri açısından **uyumluluğunu** ve sertifikanın **geçerliliğini** kontrol eden işlemler toplamıdır.

X.509 Sertifika Doğrulama

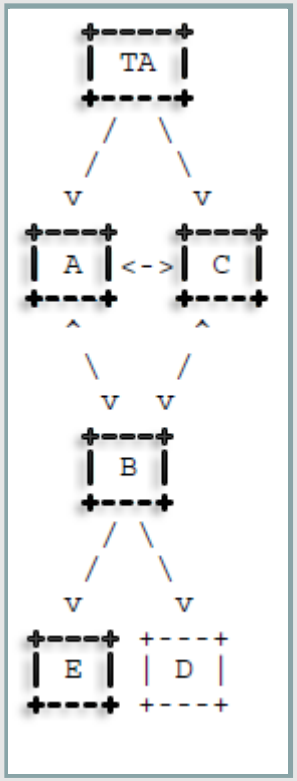
- Sertifika Zinciri Oluşturma
  (Certificate Path Building)

- Sertifika Zincir Doğrulama
  (CertificatePath Validation)

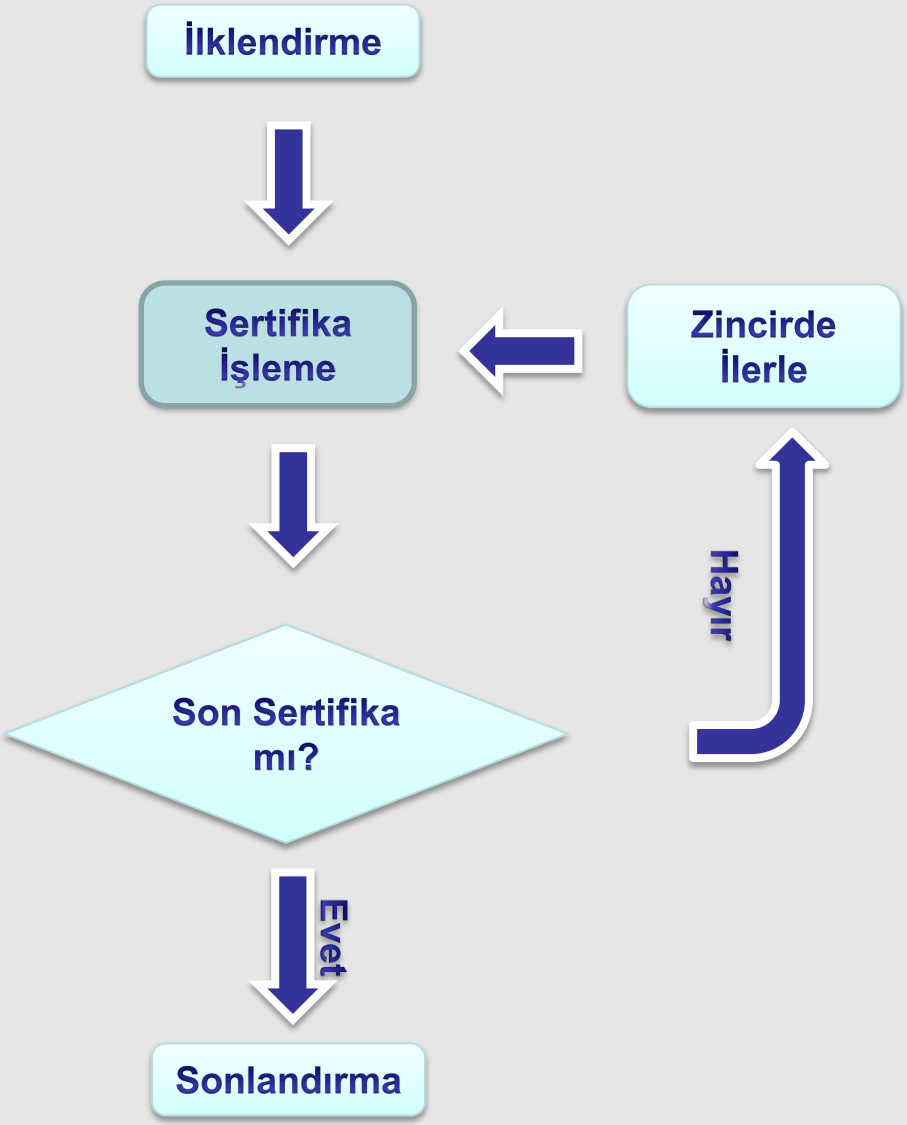


Sertifika Zinciri Oluşturma

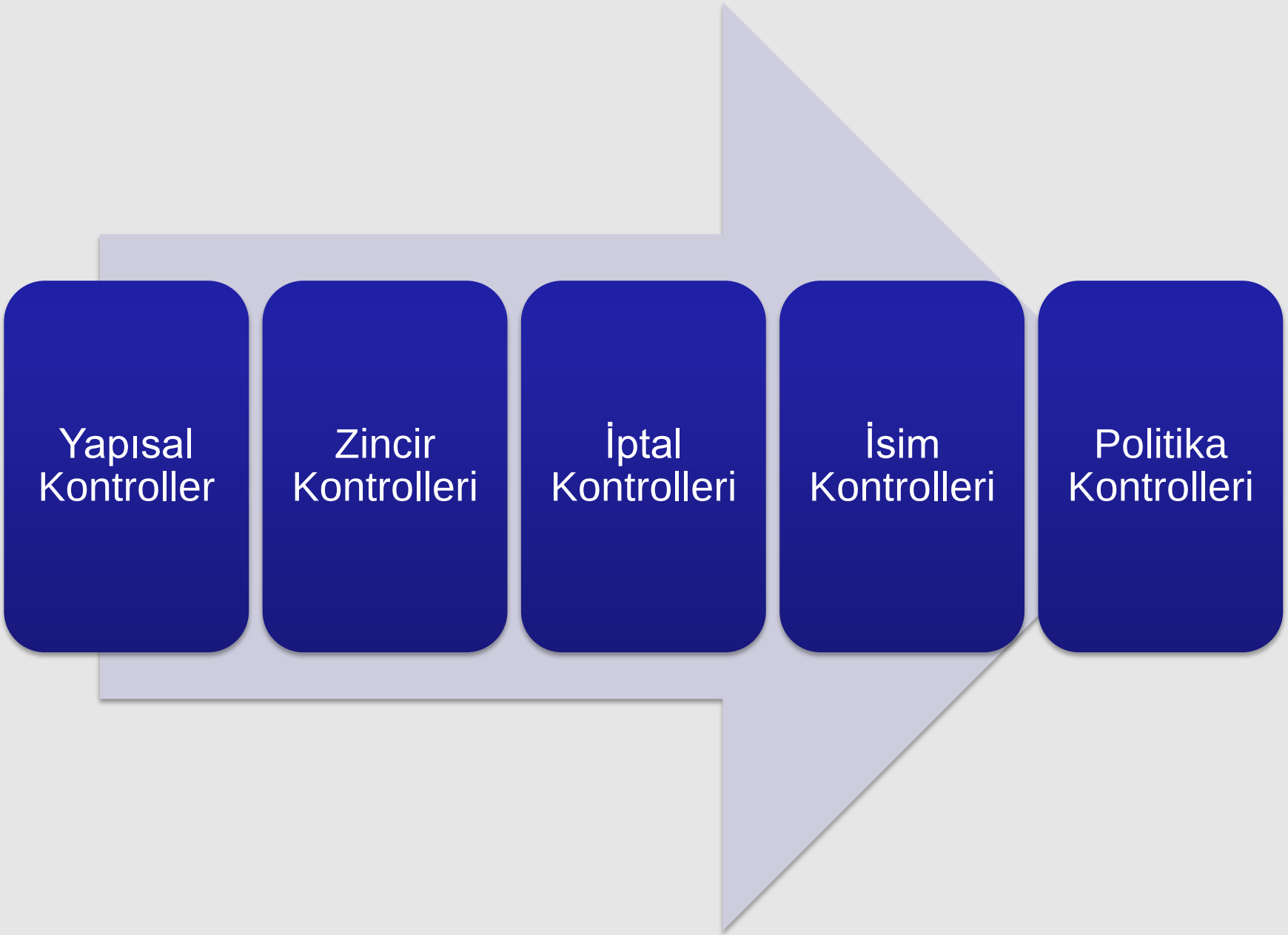
- Olası zincirlerin bulunması
  - E→B→A→TA
  - E→B→C→TA
  - E→B→C→A→TA
  - E→B→A→C→TA
  - D→B→A→TA
  - D→B→C→TA
  - …



Sertifika Zinciri Doğrulama



Sertifika İşleme



Yapısal Kontroller

Sertifikaların biçimsel özelliklerinin standartlara uygunluğunu kontrol eder.

- Sertifika Seri Numarası Kontrolü
- Sertifika Tarih Kontrolü
- Sertifika Eklentileri Kontrolü
- ..

Zincir Kontrolleri

Sertifika ile SM sertifikası arasındaki ilişkilerin doğruluğunu kontrol eder

- Sertifika imzası
- Yol uzunluğu
- Anahtar kullanımı
- Temel kısıtlar
- ..

İptal Kontrolleri

Sertifikanın iptal durumunu kontrol eder.

- SİL'den iptal durumu kontrolü
- OCSP'den iptal durumu kontrolü

İsim ve Politika Kontrolleri

- İsim Kontrolleri

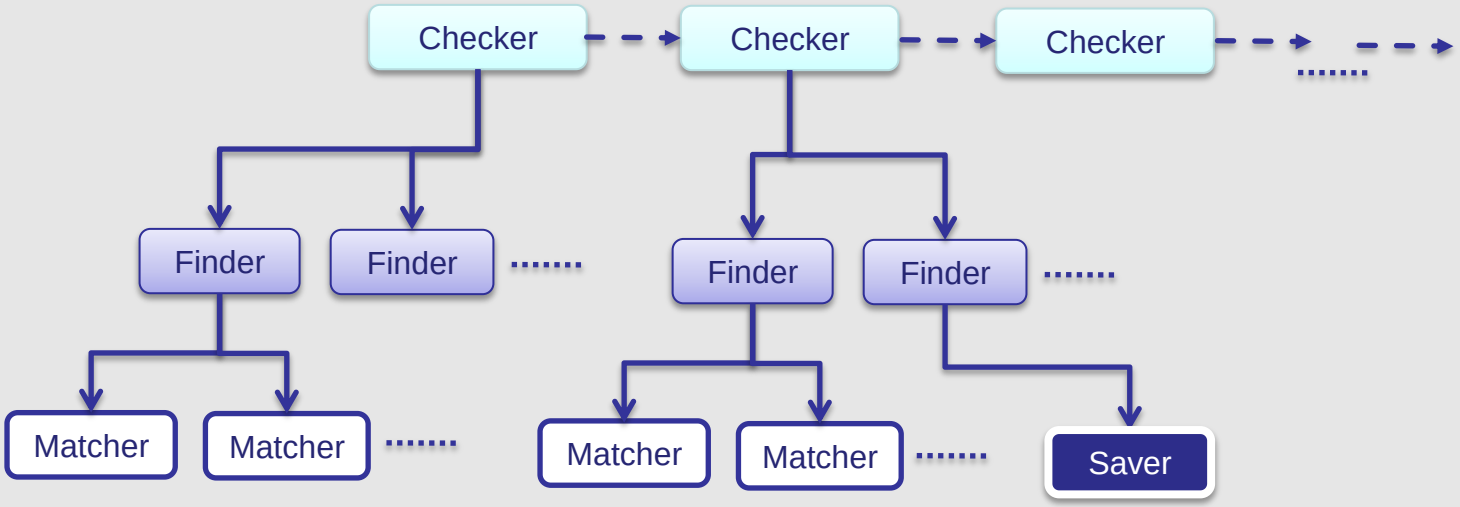
  Sertifika özne adı ile yayıncı sertifikasındaki **isim kısıtları** uyumluluk kontrolleri

- Politika Kontrolleri

  Sertifika politikaları adı ile yayıncı sertifikasındaki **politika kısıtları** uyumluluk kontrolleri

ESYA API Sertifika Doğrulama Modülleri

- Bulucular (Finder)
- Kontrolcüler (Checker)
- Eşleştiriciler (Matcher)
- Kaydediciler(Saver)
- Sertifika Doğrulama Politikası (CertificateValidationPolicy)
- Sertifika Doğrulama Sonuç Bilgisi(CertificateStatusInfo)



Kontrolcüler (Checker)

- Sertifika Kontrolcüler (CertificateChecker)
  - Tek Sertifika Kontrolcüler
  - SM Sertifika Kontrolcüleri
- İptal Durumu Kontrolcüler (RevocationChecker)
- SİL Kontrolcüler (CRLChecker)
- OCSP Cevabı Kontrolcüler (OCSPResponseChecker)

Bulucular(Finder)

- Güvenilir Sertifika Bulucular
- Sertifika Bulucular
- Çapraz Sertifika Bulucular
- SİL Bulucular
- DeltaSİL Bulucular
- OCSP Cevabı Bulucular

Eşleştiriciler(Matcher)

- Sertifika Eşleştiriciler
- Çapraz Sertifika Eşleştiriciler
- SİL Eşleştiriciler
- Delta SİL Eşleştiriciler
- OCSP Cevabı Eşleştiriciler

Kaydediciler(Saver)

- Sertifika Kaydediciler
- SİL Kaydediciler

Sertifika Doğrulama Politikası

- XML dosyası ile tanımlanabilir (Politika Dosyası)
- Dinamik olarak oluşturulabilir (ValidationSystem)

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

<policy>
      <find>
        <trustedcertificate>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.find.certificate.trusted.TrustedCertificateFinderFromECertStor
          <param name ="securitylevel" value="legal;organizational;personal"/>
          </class>
        </trustedcertificate>
        <certificate>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.find.certificate.CertificateFinderFromECertStore">
          </class>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.find.certificate.CertificateFinderFromLDAP">
          <param name ="remote" value="true"/>
          </class>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.find.certificate.CertificateFinderFromHTTP">
          <param name ="remote" value="true"/>
          </class>
        </certificate>
        <deltacrl>
        </deltacrl>
      </find>
      <match>
        <certificate>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.match.certificate.IssuerSubjectMatcher"/>
        </certificate>
        <crl>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.match.crl.CRLIssuerMatcher"/>
        </crl>
        <deltacrl>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.match.deltacrl.BaseCRLNumberMatcher"/>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.match.deltacrl.CRLNumberMatcher"/>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.match.deltacrl.DeltaCRLIssuerMatcher"/>
          <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.match.deltacrl.ScopeMatcher"/>
        </deltacrl>
      </match>
      <validate>
        <certificate>
          <self>
            <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.check.certificate.self.SignatureAlgConsistencyChecker"/>
            <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.check.certificate.self.PositiveSerialNumberChecker"/>
            <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.check.certificate.self.CertificateExtensionChecker"/>
            <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.check.certificate.self.CertificateDateChecker"/>
            <class name = "tr.gov.tubitak.uekae.esya.api.certificate.validation.check.certificate.self.VersionChecker"/>
```

Güvenli Kullanım

- Politika Dosyası
  - Bilinçli bir şekilde yapılandırılmalı
  - Yetkisiz erişim engellenmelidir
  - Gerekirse imzalı saklanıp doğrulanmalı

- Güvenilir Kök Deposu güvenli ortamda saklanmalı ve güncel tutulmalı
- Mümkünse OCSP ile iptal kontrolü tercih edilmeli
- Yeni kontrolcü,bulucu vb. sınıf gerçeklemelerinde standartlara uygunluk göz önünde bulundurulmalı

Örnek Kod

- **Java**

```
ValidationSystem vs =
CertificateValidation.createValidationSystem(policy);
vs.setBaseValidationTime(Calendar.getInstance());
CertificateStatusInfo csi =
CertificateValidation.validateCertificate(vs, cert);
```

- **C#**

```
ValidationSystem vs =
CertificateValidation.createValidationSystem(policy);
vs.setBaseValidationTime(DateTime.UtcNow);
CertificateStatusInfo csi =
CertificateValidation.validateCertificate(vs, cert);
```

Sorular

İletişim :
Tel : (0262) 648 1000 Faks : (0262) 648 1100 e-posta :bilgi@kamusm.gov.tr