ESYA E-imza Kütüphaneleri

Murat Yasin Kubilay
Milli Açık Anahtar Altyapısı (MA3) Proje Yöneticisi

Nisan 2012, Ankara

Gündem

- E-İmza Tanımı ve Çeşitleri
- ESYA E-İmza Kütüphaneleri
- E-İmza Kütüphanelerinin Uyumu
- E-İmza Çalışmalarımız

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"*

- Bir kimsenin elektronik ortamdaki
  - *Bir metni onayladığını*
  - *Bir anlaşmayı veya sözleşmeyi kabul ettiğini*

  belirtmek için elektronik imza üretme aracıyla ürettiği elektronik veridir.

- Elektronik imza, imza sahibinin kimliğini imzalanan veriyle ilişkilendirir ve imzalanan verinin değiştirilmediğini ispat eder.

E-İmza Çeşitleri Nelerdir ?

E-İmza Türü	İlgili Standart
CAdES(CMS Advanced Signature)	ETSI TS 101 733 V1.8.1
XAdES (XML Advanced Signature)	ETSI TS 101 903 V1.4.2
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

E-İmza Tipleri	Açıklama
BES	Basit Elektronik İmza
EPES	Belirlenmiş Politika Temelli Elektronik İmza
ES-T	Zaman Damgalı Elektronik İmza
ES-C	Doğrulama Verisi Taşıyan Elektronik İmza
ES-X	Genişletilmiş Elektronik İmza
ES-XL	Genişletilmiş Uzun Elektronik İmza
ES-A	Arşiv Elektronik İmza

E-İmza Kullanımı Hızla Artıyor...

- E-imzalı ortak yazışma paketi

  BAŞBAKANLIK İdareyi Geliştirme Başkanlığı: **Resmî Yazışmalarda Uygulanacak Usul ve Esaslar Hakkında Yönetmelik**

  E-imzalı belge üretilmesi için gerekli çalışmalar **31.12.2012**, belge paylaşımı için gerekli çalışmalar **30.06.2013** tarihi itibariyle tamamlanacaktır. Islak imzalı belge gönderilmeyecektir.

  KALKINMA BAKANLIĞI Bilgi Toplumu Dairesi: **E- yazışma Teknik Rehberi** (*http://www.e-yazisma.gov.tr/*)

  Üst yazı, ekler, üst veri elemanları ve e-imzayı barındıran paket yapısını tanımlamaktadır.

  Paketin gizliliğini sağlamak amacıyla şifrelenmesinin nasıl yapılacağını tanımlamaktadır.

  Pakete elektronik mühürün nasıl alınacağını tanımlamaktadır. (E-mühür henüz yasal olarak düzenlenmemiştir)

- Paketin gönderimi (Kayıtlı e-posta sistemi- KEP)

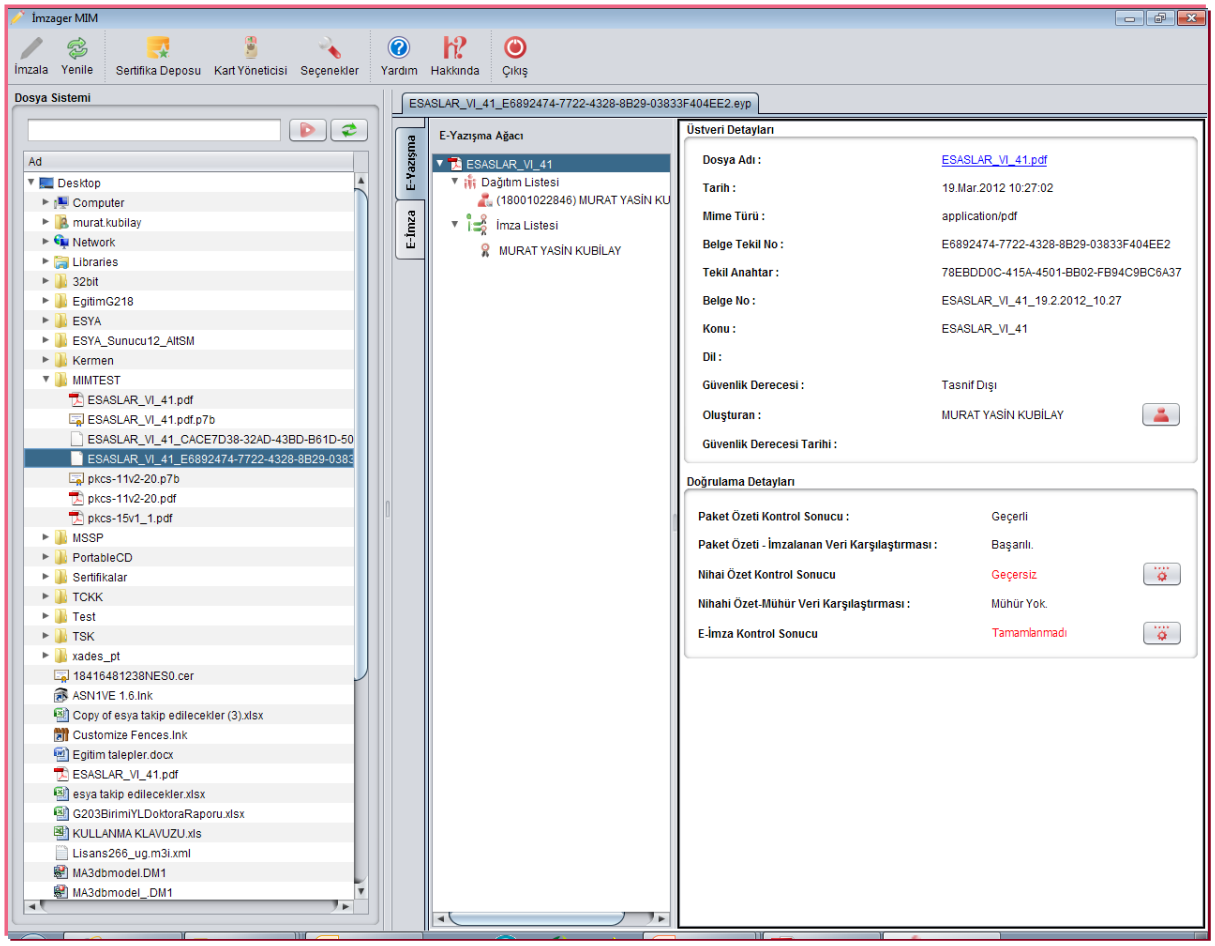
Tübitak E-İmza Kütüphaneleri

Tür	Java	.NET	Yayın Tarihi (İmzager)	Yayın Tarihi (ESYA)
CADES	+	+	2006	2011
XADES	+	-	-	2011
PADES	-	-	-	-

Yeni E-İmza Kütüphanesi (ESYA)

- Türkiye'de geliştirilmiş tek milli e-imza kütüphanesidir.
- Object Oriented Tasarım, Esnek Konfigürasyon Yapısı
- Yaklaşık 50 farklı uluslararası e-imza kütüphanesinin birlikte çalışabilirlik testlerinin yapıldığı ETSI plug testlerine 3 kez katılım ve kütüphanelerin standartlara uygunluğunun tespiti
- NIST'in 150 sertifika doğrulama test adımı ile standartlara uygunluk kontrolü
- SHA-2 ve EC desteği
  - ETSI TS 102 176-1, RSA 1024 anahtar boyunu ve SHA-1 özet algoritmasını tavsiye listesinden çıkardı
  - Microsoft
- Örnek kodlar / Applet / ActiveX (Daha da gelişecek)
- Detaylı Kullanım Kılavuzu
- JavaDoc / Doxygen (Yeterli Değil !!! Hızla iyileşecek)

Yeni İmzager MİM



- E-Yazışma formatı desteği
- CADES desteği
- XADES desteği (eklenecek)
- ASIC desteği (eklenecek)
- Mobil İmza desteği (eklenecek)

E-İmza Kütüphanesinin Güncellenmesi

- Tüm İmzager E-İmza kütüphanesi kullanıcıları yazılım güncellemesi yapmalı...

- Çünkü BTK, '*Elektronik İmza ile ilgili süreçlere ve Teknik Kriterlere İlişkin Tebliğ*' de düzenleme yaparak elektronik imza özet algoritmalarından SHA-1 ve RIPEMD'yi çıkartmayı planlamaktadır. **31 Ekim 2012** tarihine kadar e-imza uygulamalarına SHA-2 desteği eklenmesini istemektedir.

- Öncelikli tercih, tüm İmzager kütüphanesi kullanıcılarının ESYA kütüphanesine geçmesi

- Mümkün değilse, İmzager kütüphanesinin yeni sürümüne geçilmeli

Türkiye için Plugtestler

- Türkiye'de kullanılan e-imza kütüphanelerinin standartlara uyumu
- E-imza kütüphanelerinin birlikte çalışabilirliği
- **Haziran** Ayında Türkiye'de kullanılan e-imza kütüphaneleri için plugtestler düzenlenecektir.
- Plugtest'lerde farklı imza formatlarının oluşturulması, imzaların dönüştürülmesi, sertifika doğrulama senaryoları test edilecek ve sonuçlar rapor olarak yayınlanacaktır.

E-İmza Çalışmalarımız (Teknoloji)

- Yaklaşık 50 farklı uluslararası E-imza kütüphanesinin birlikte çalışabilirlik testlerinin yapıldığı ETSI plug testlerine 3 kez katılım ve kütüphanelerin standartlara uygunluğunun tespiti
- ETSI – ESI (Electronic Signature) 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 ve 7 kurum (Cumhurbaşkanlığı, Başbakanlık, DPT vs) arasında yürütülen pilot projede E-imza, Şifreleme kütüphanelerinin sağlanması ve desteğinin verilmesi

E-İmza Çalışmalarımız (Denetim)

- 19 Nisan 2006, 2006/13 sayılı, Kamu Sertifikasyon Hizmetlerine İlişkin Usul ve Esaslar konulu Başbakanlık Genelgesi:
  - İş süreçleri ve uygulama yazılımları e-imza kullanımına uygun hale getirilmiş bilgi sistemleri test sertifikaları kullanılarak denenecektir. Sistemin uluslararası standartlara uygun çalıştığı Kamu SM tarafından doğrulandıktan sonra sertifika üretim süreci başlatılacaktır.
- İmza oluşturma ve doğrulama yazılımları toplam 129 maddelik "Kontrol Listesi" üzerinden kontrol edilmektedir.
  - ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES)
  - ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)
  - CWA 14170: Security Requirements for Signature Creation Applications
  - CWA 14171: Procedures for Electronic Signature Verification
  - Türkiye'deki E-imza Mevzuatı
- 2007 yılından itibaren 47 kamu kurumu ve 5 özel kurumun e-imza uygulamaları incelenmiştir.
- Kontroller her e-imza uygulaması için ayrı yapılmakta ve sonrasında kuruma rapor yazılıp gönderilmektedir.
- Gelecekteki çalışma:
  - Kontrollerin daha detaylı yapılması için yeni bir test paketi ve prosedürler oluşturulmaktadır.

E-İmza Çalışmalarımız (Destek)

- *https://yazilim.kamusm.gov.tr* adresinden kütüphanelerin yayınlanması, sürümlere hızlı erişim, toplam 275 kayıtlı kullanıcı
- *https://mi.kamusm.gov.tr* adresinden online hata ve geri bildirim takibi, 1000'den fazla biletin sonuçlandırılması
- Kurumlara e-imza süreçlerinin anlatılması
- Yazılım geliştiricilere telefonla destek verilmesi
- Farklı kurumlarda atılan e-imzaların standartlara uygunluğunun kontrolü
- E-İmza Kütüphanesi Eğitimleri

E-İmza Çalışmalarımız (Hedeflenen)

- E-İmza yaşam döngüsü gerçeklenmeli
- Tübitak E-İmza kütüphanesi satışı, entegrasyonu, desteği özel yazılımevleri tarafından yapılacak.
  - İlk özel şirket …
- Kütüphaneler hakkındaki her türlü destek yazılımevlerine sağlanacak

Sorular