



Elektronik İmza ve Güvenlik

Ersin GÜLAÇTI

Kamu Sertifikasyon Merkezi Yöneticisi

Mart, 2008

TASNİF DIŞI

- **Elektronik imza nedir?**
- **Elektronik imza neden daha güvenlidir?**
- **E-devlet uygulamalarında e-imza kullanımı**
- **İmzager yazılımı tanıtımı**



Elektronik İmza Nedir?

5070 Sayılı Elektronik İmza Kanunu:

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

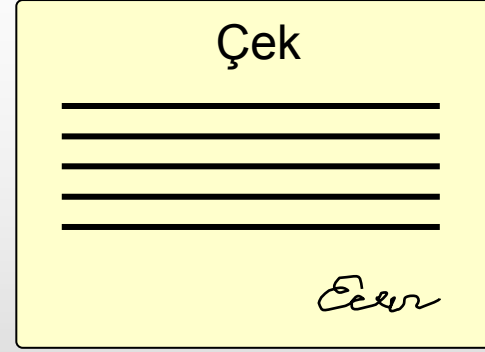
Elektronik İmza Neleri Sağlar?

- Bilgi bütünlüğü
- Kimlik doğrulama
- İnkâr edilemezlik

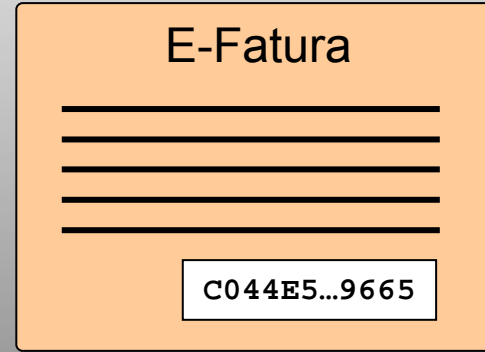
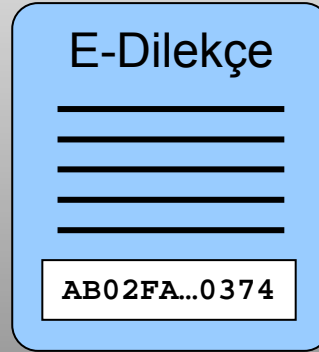
Elektronik imza, imza sahibinin kimliğini imzalanan veriyle ilişkilendirir ve imzalanan verinin değiştirilmediğini ispat eder.

Elektronik İmzanın Islak İmzadan Farkı

Islak imza örnekleri



Elektronik imza örnekleri

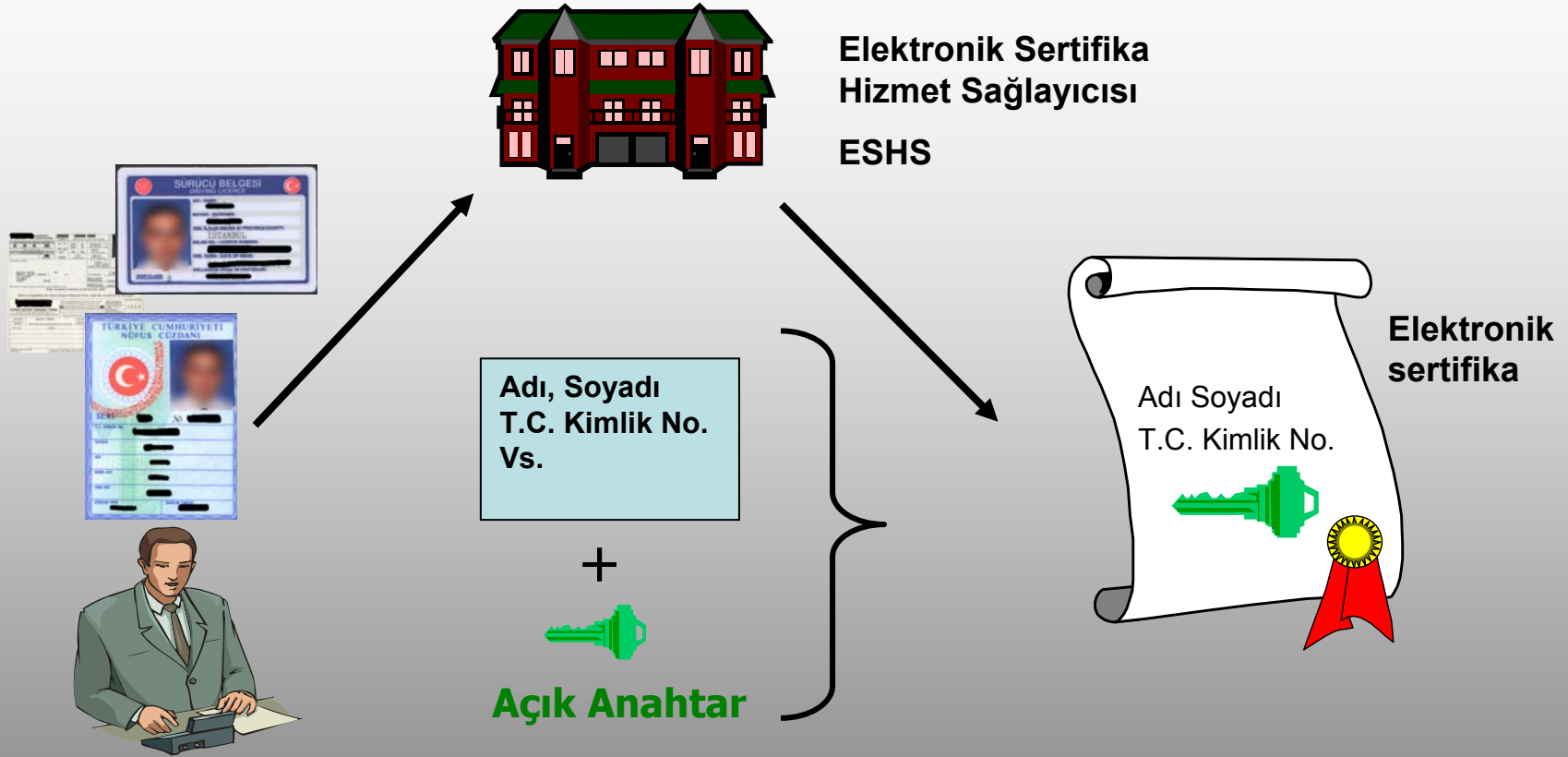


Elektronik imza, imzanın atıldığı belgenin içeriği de kullanılarak oluşturulur.

Açık Anahtarlı Altyapı teknolojisi (AAA-PKI)

- Her kullanıcıya 2 anahtar verilir:
 - Özel anahtar (imza oluşturma verisi)
 - Açık anahtar (imza doğrulama verisi)
- Çift anahtarlı (asimetrik) bir algoritma kullanılır (RSA, DSA, ECDSA vs..)
- Özet algoritması kullanılır (SHA, RIPEM, vs..)

Elektronik Sertifikalar



Elektronik Sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır

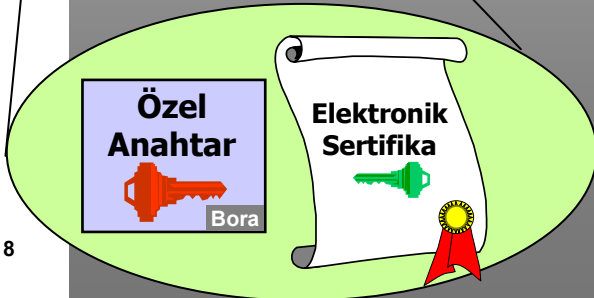
E-imzalı Belge Oluşturma

Elektronik İmzalı Bir Belge Nasıl Oluşturulur?

Bora



Güvenli Elektronik İmza Oluşturma Aracı



Belge
Ankara'daki
12204 no'lu
hesabıma
1,000 YTL
gönder

**Özetleme
Algoritması**

Mesaj Özeti

**İmzalama
Algoritması**

**Elektronik
İmza**



E-imzalı Belge

Belge

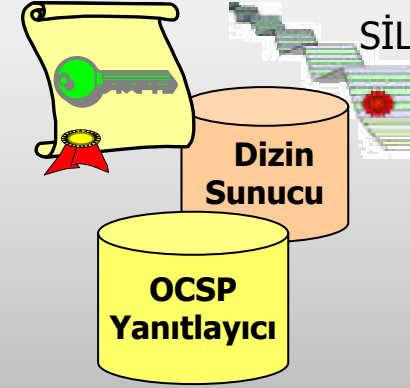
Ankara'daki
12204 no'lu
hesabıma
1,000 YTL
gönder

Elektronik İmza

**Elektronik
Sertifika**

Elektronik Sertifikanın Doğrulanması

Elektronik Sertifika
Hizmet Sağlayıcısı
ESHS



- Elektronik Sertifika Hizmet Sağlayıcısının imzası
- Elektronik sertifikanın geçerlilik süresi
- Sertifikanın kullanım amacının uygunluğu
- Sertifikanın iptal olup olmadığı

Elektronik İmza Neden Daha Güvenli?

- İmza taklidini çok zor hale getiriyor
- İmza oluşturma ve doğrulama işlemlerini, teknolojik araçların kullanıldığı süreçlere dönüştürüyor (öznel yöntemler yerine nesnel yöntemler kullanılıyor)
- İmzalanan verinin sonradan değiştirilmediğini ispata yarıyor
- İmzalanan veriyi kimin imzaladığını kanıtlıyor
- İmza atacak kişinin kimlik doğrulaması güvenilir sertifika hizmet sağlayıcıları tarafından sertifika verilirken yapılıyor

- 5070 Sayılı Elektronik İmza Kanunu, **Ocak 2004**
- 5070 Sayılı Kanunun Yürürlüğe Girmesi, **Temmuz 2004**
- 2004/21 Başbakanlık Genelgesi, Kamu Sertifikasyon Merkezinin Oluşturulması, **Eylül 2004**
- UEKAE’nin İlk Sertifikayı Vermesi, **Temmuz 2005**

E-devlet için E-imza Kullanımı

80 Nitelikli Elektronik Sertifika talepleri üzerine uygulama analizi gerçekleştirilen kurum sayısı

52 İmza yazılım kütüphanelerinin kullanımına sunulduğu kurum ve kuruluş sayısı

7 Tamamlanmış e-imza uygulaması incelenerek mevzuata ve uluslararası standartlara uygun olarak çalıştığı tespit edilen kurum sayısı

14,000

Verilmiş olan nitelikli elektronik sertifika sayısı

Nitelikli Elektronik Sertifika Kullanımı

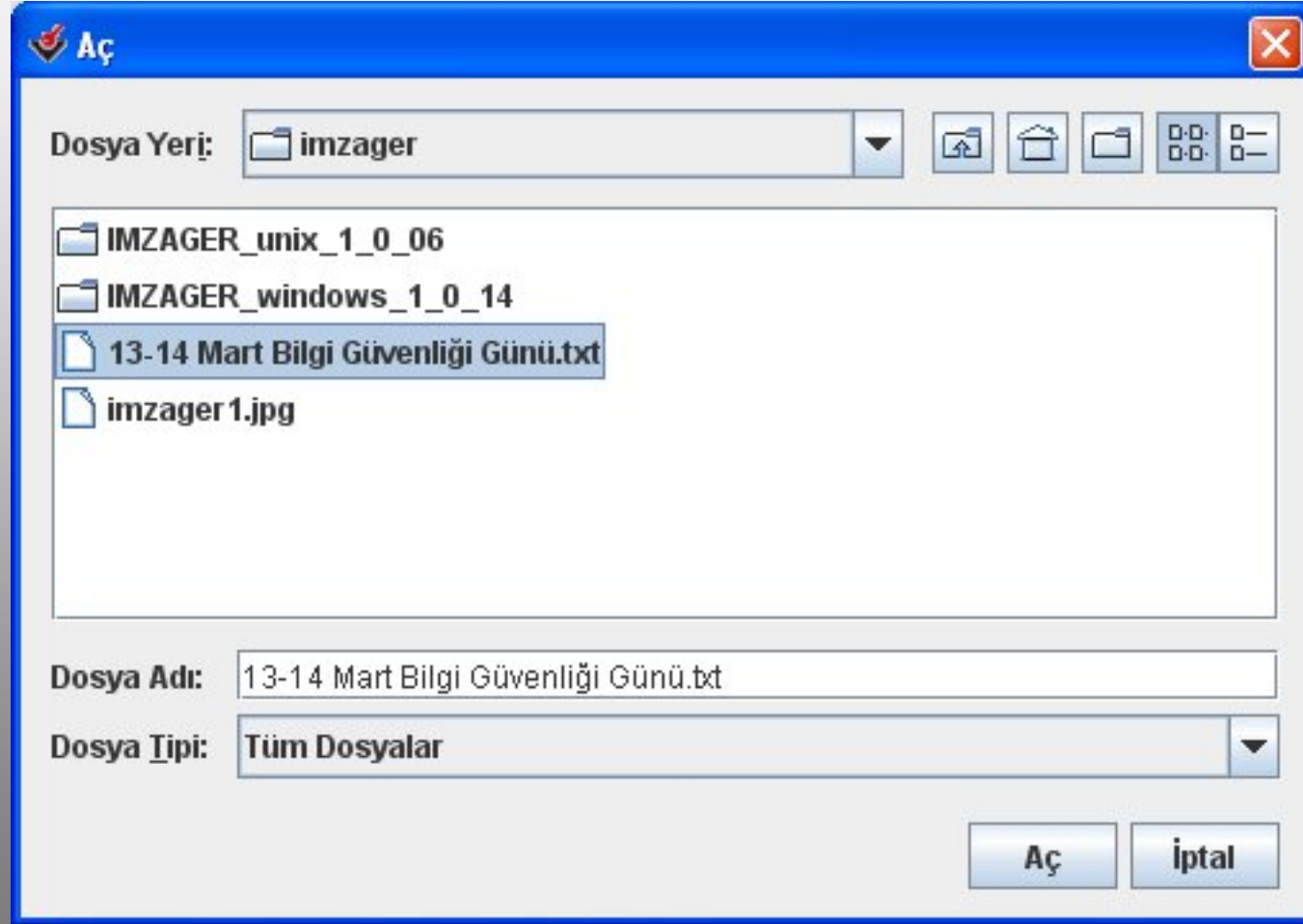
| Kurum Adı | Toplam |
|---|--------------|
| ADALET BAKANLIĞI | 6.643 |
| TÜBİTAK | 1.174 |
| TCDD | 1.164 |
| DEVLET SU ISLARI | 779 |
| BANKACILIK DÜZENLEME VE DENETLEME KURUMU | 505 |
| TELEKOMÜNİKASYON KURUMU BASKANLIĞI | 483 |
| GÜMRÜK MÜSTESARLIĞI | 461 |
| DIŞ TİCARET MÜSTEŞARLIĞI | 375 |
| TÜRKİYE PETROLLERİ A.O. | 300 |
| TÜRKİYE İSTATİSTİK KURUMU | 290 |
| TÜRKİYE İŞ KURUMU | 284 |
| T.C. BAYINDIRLIK VE İSKAN BAKANLIĞI | 240 |
| MSB SAVUNMA SANAYİ MÜSTEŞARLIĞI | 235 |
| DIŞ TİCARET MÜSTEŞARLIĞI - SERBEST BÖLGELER | 216 |
| DEVLET MALZEME OFİSİ GENEL MÜDÜRLÜĞÜ | 186 |
| MALİYE BAKANLIĞI MASAK | 136 |
| T.C. KOCAELİ BÜYÜKŞEHİR BELEDİYE BAŞKANLIĞI | 103 |
| BAKIRKÖY İLÇE MİLLİ EĞİTİM MÜDÜRLÜĞÜ | 63 |
| İSKİ | 60 |
| SANAYİ VE TİCARET BAKANLIĞI | 50 |

Güvenilir imza doğrulama işlemlerinde referans olarak kullanılacak bir araç sunmak.



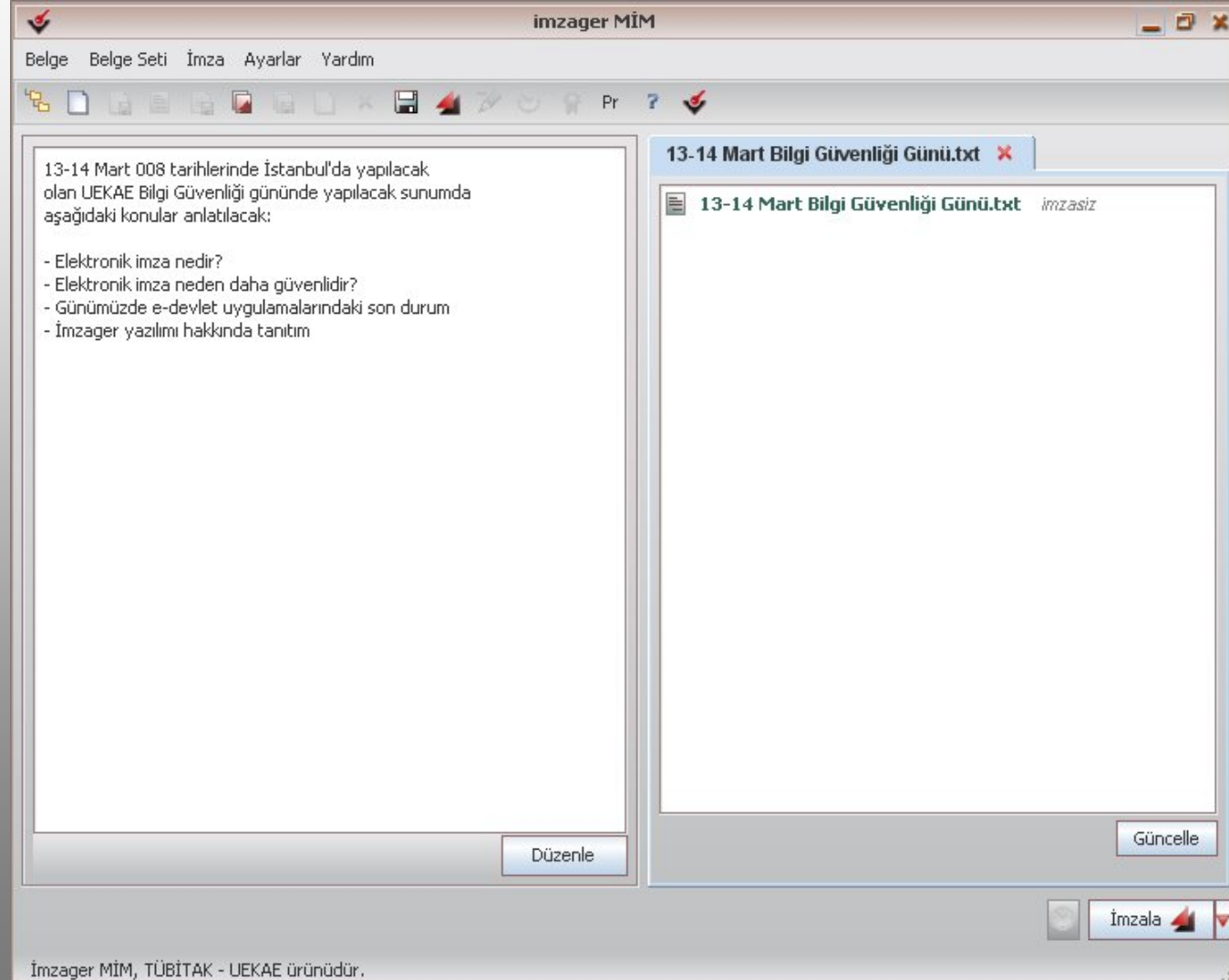
- **ETSI 101733 standardına uyumlu**
 - Seri imza atma
 - Zaman damgası alma
 - Basit, gelişmiş, arşiv imzası doğrulama
 - Seri-paralel imza doğrulama
- **Java tabanlı, platform bağımsız**
- **KamuSM sertifikaları ile imza atma, tüm nitelikli imzaları doğrulama**

Bir dosya seçelim

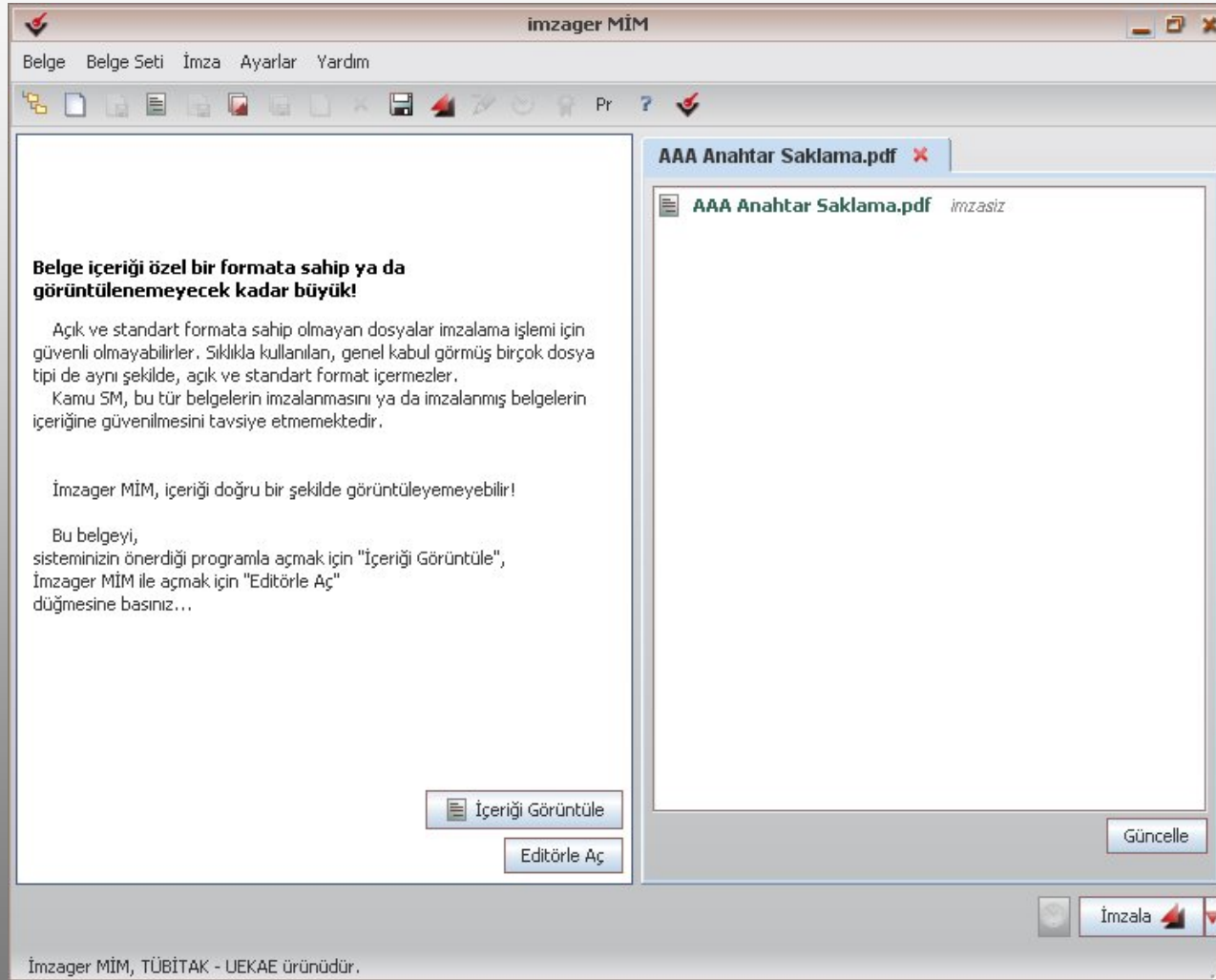


İmzager Kullanımı

Bilinen bir içerik (txt, zmf, jpg, tif, gif) görüntülenir



Bilinmeyen içerik için uyarı verilir



Akıllı kart parola giriş ekranı açılır



PIN Giriş

Seçili Sertifika
ERSİN GÜLAÇTI

Görüntüle Seç

Akıllı kart PIN kodunu giriniz...

1 2 3
4 5 6
7 8 9
0 <Sil

Rakamları karıştır

Tamam İptal

İstenirse sertifika görüntülenir

Sertifika - ERSİN GÜLAÇTI

Sertifika | Ayrıntılar | Sertifika Zinciri | Kaydet

Nitelikli İmza Sertifikası

Adı: ERSİN GÜLAÇTI
T.C. Kimlik No: 3 [REDACTED] 8

Üretici: Kamu Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 3
Başlangıç Tarihi: 18 Ekim 2007 Perşembe 10:19:03
Bitiş Tarihi: 17 Ekim 2010 Pazar 10:19:03
Seri No: 22 40
Kullanım Amaçları: Sayısal İmza Oluşturma, İnkâr Edilemezlik
Maddi Sınır: 0 YTL

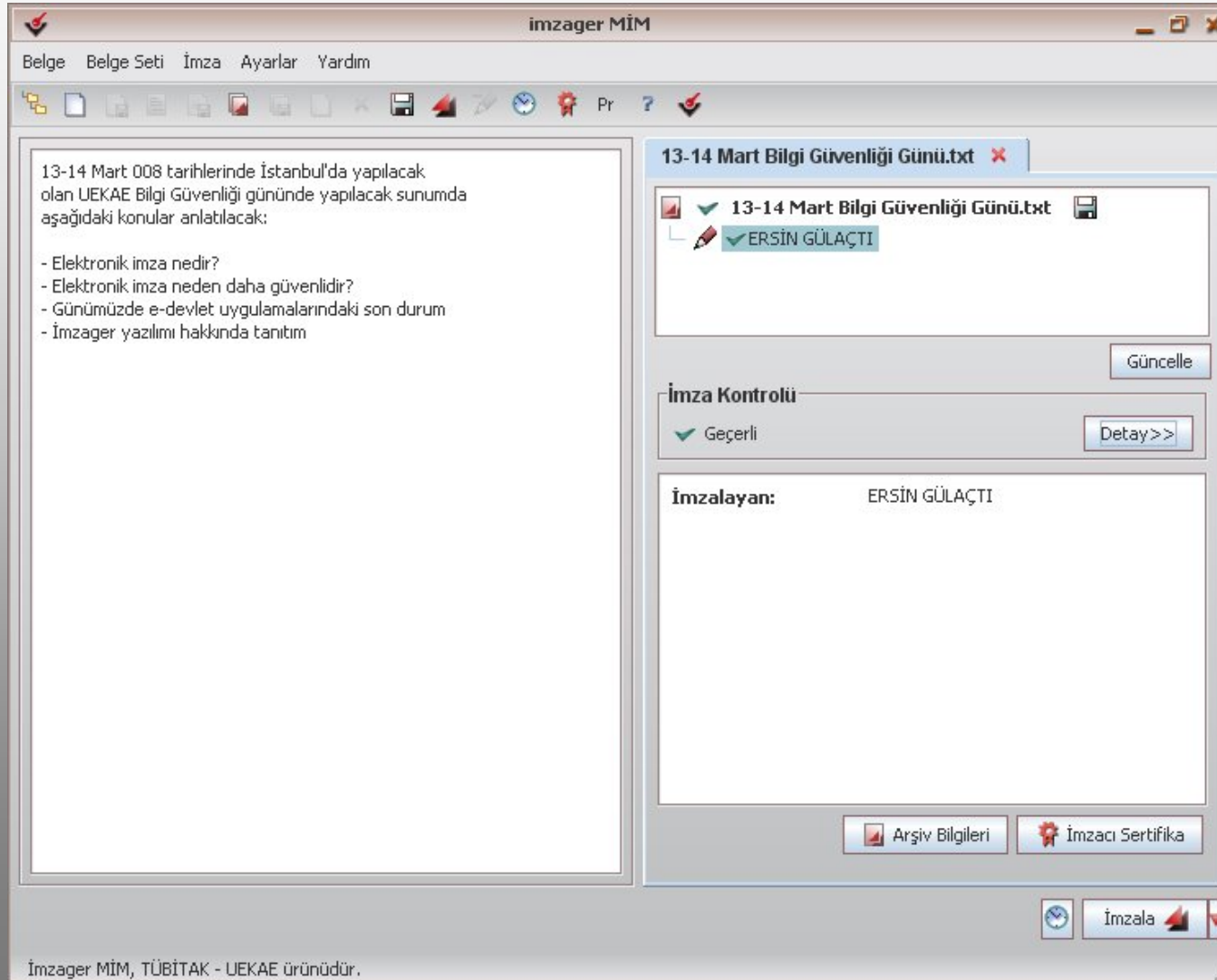
Sertifika yaşamı

18.10.2007 [Progress Bar] 17.10.2010
10.3.2008
%13,15

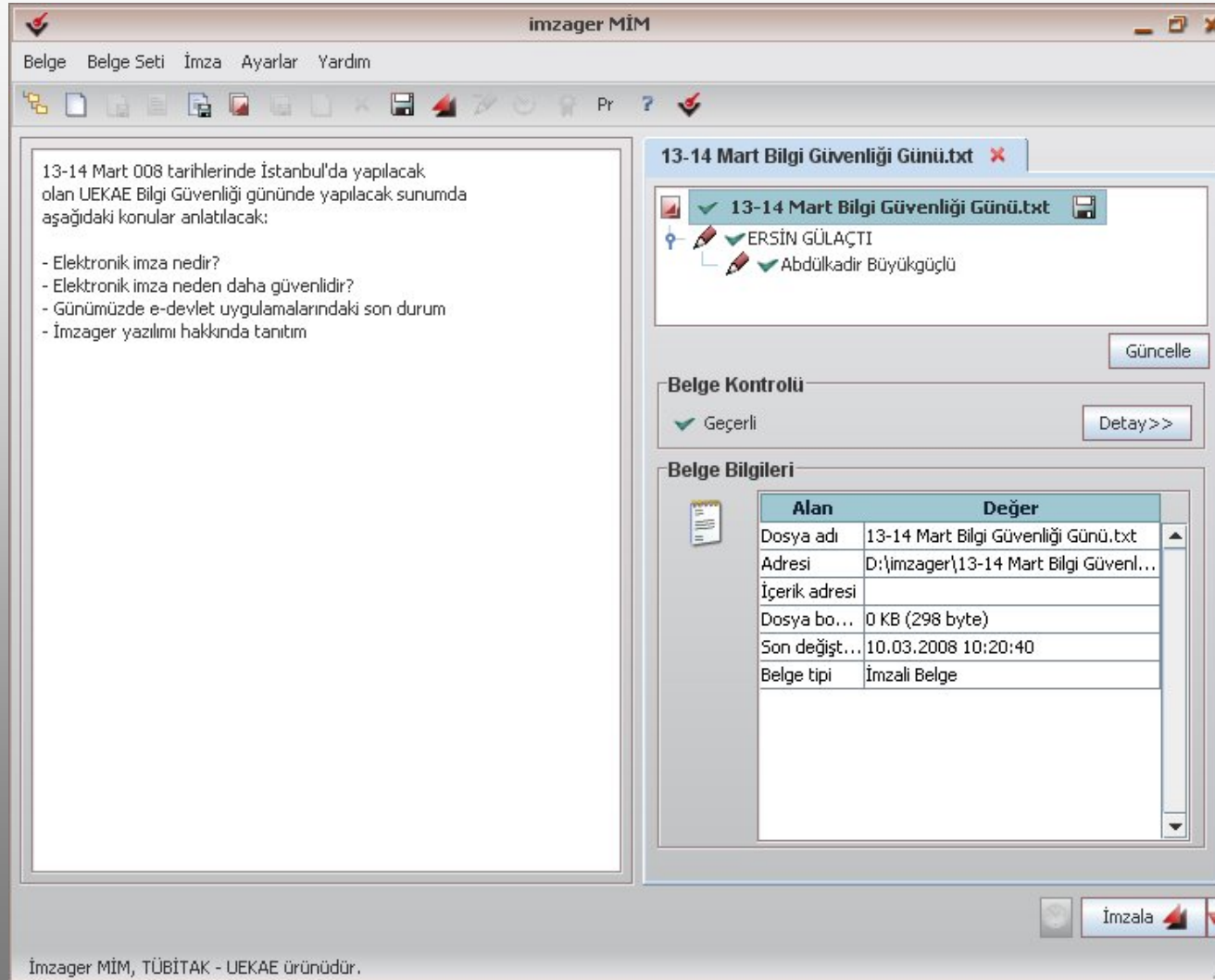
Başlangıç tarihinden itibaren geçen süre: 4 ay 24 gün

✓ Sertifika geçerli [Detay >>](#)

İmza oluşturulur ve “imz” uzantılı olarak kaydedilir



Çoklu imzalar atılabilir



The screenshot displays the İmzager MİM application window. The main text area contains the following content:

13-14 Mart 008 tarihlerinde İstanbul'da yapılacak olan UEKAE Bilgi Güvenliği gününde yapılacak sunumda aşağıdaki konular anlatılacak:

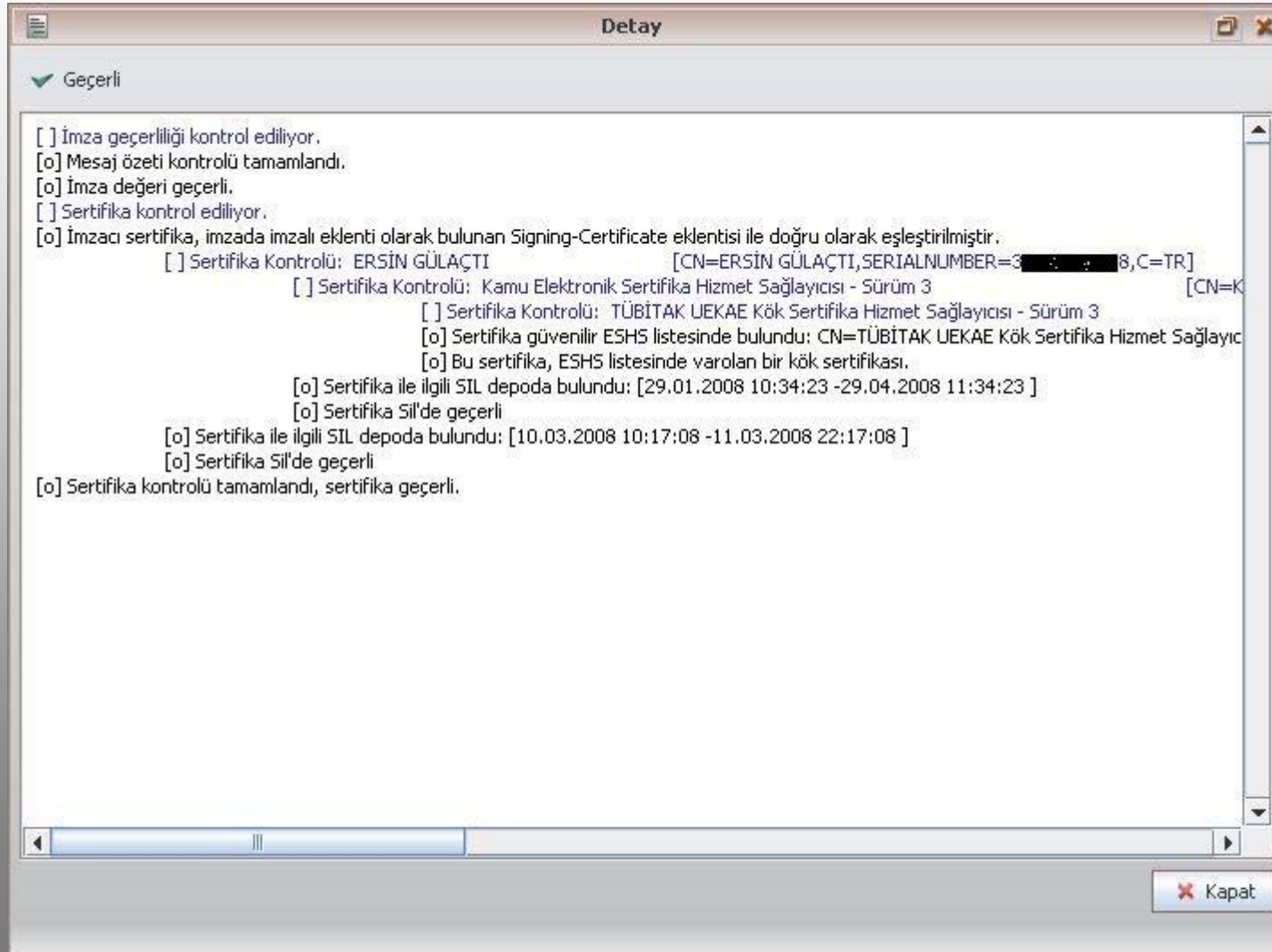
- Elektronik imza nedir?
- Elektronik imza neden daha güvenlidir?
- Günümüzde e-devlet uygulamalarındaki son durum
- İmzager yazılımı hakkında tanıtım

The right-hand side of the interface shows the document details for "13-14 Mart Bilgi Güvenliği Günü.txt". It lists two signatures: ERSİN GÜLAÇTI and Abdülkadir Büyükgüçlü. Below this, the "Belge Kontrolü" section indicates the document is "Geçerli" (Valid). The "Belge Bilgileri" section provides a table of document metadata:

| Alan | Değer |
|---------------|---------------------------------------|
| Dosya adı | 13-14 Mart Bilgi Güvenliği Günü.txt |
| Adresi | D:\İmzager\13-14 Mart Bilgi Güvenl... |
| İçerik adresi | |
| Dosya bo... | 0 KB (298 byte) |
| Son değişt... | 10.03.2008 10:20:40 |
| Belge tipi | İmzalı Belge |

At the bottom of the window, there is a button labeled "İmzala" (Sign) and a footer text: "İmzager MİM, TÜBİTAK - UEKAE ürünüdür."

İmzanın kontrolü ile ilgili detaylı bilgi alınabilir



Sorular

