TÜBİTAK
UEKAE

Elektronik İmza ve Güvenlik

Ersin GÜLAÇTI
Kamu Sertifikasyon Merkezi Yöneticisi

Mart, 2008

TASNİF DIŞI

Konular

- 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:

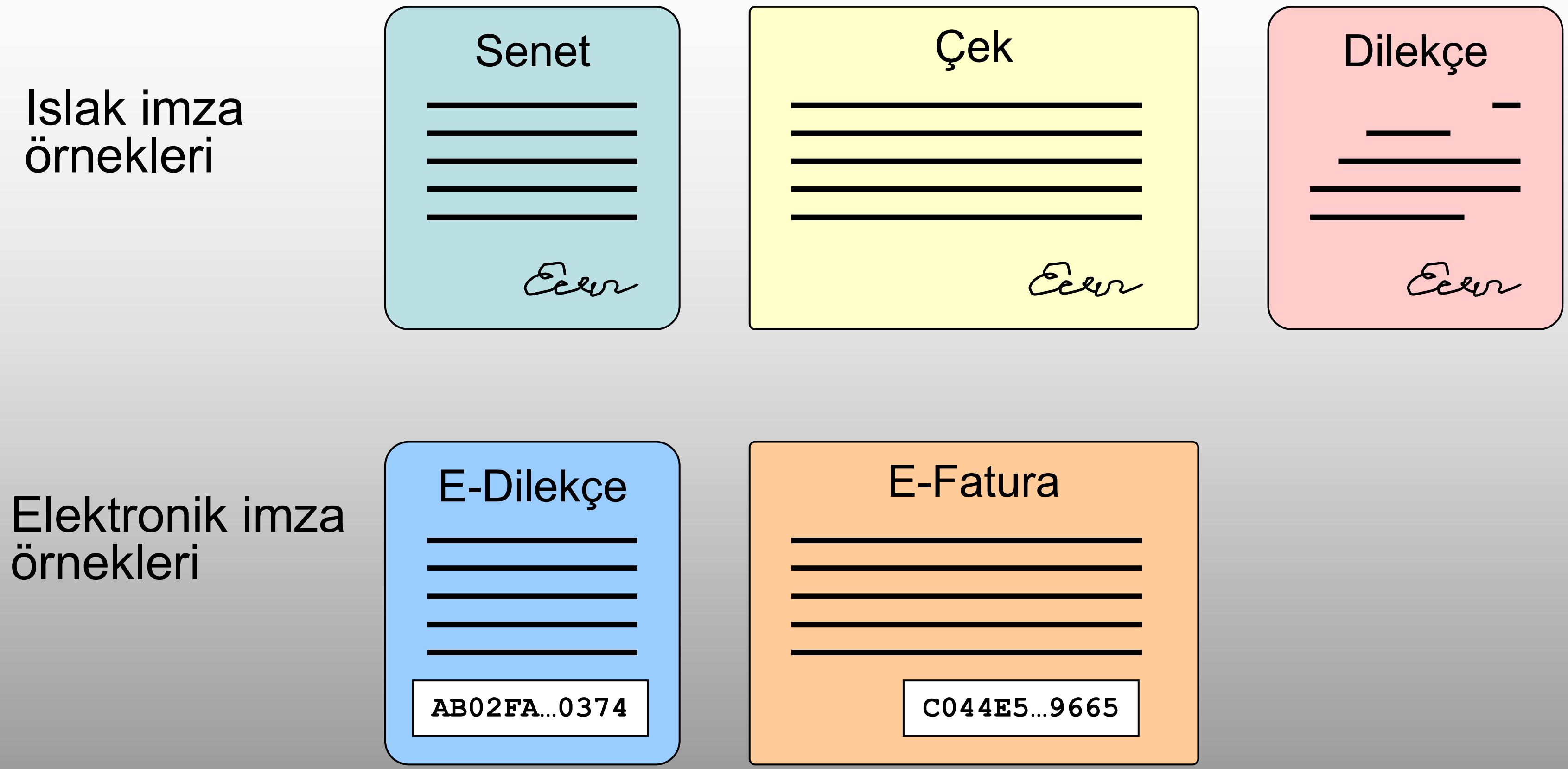
“Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri”

Elektronik İmza Neleri Sağlar?

- Bilgi bütünlüğü
- Kimlik doğrulama
- İnkar edilemezlik

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

Elektronik İmzanın Islak İmzadan Farkı



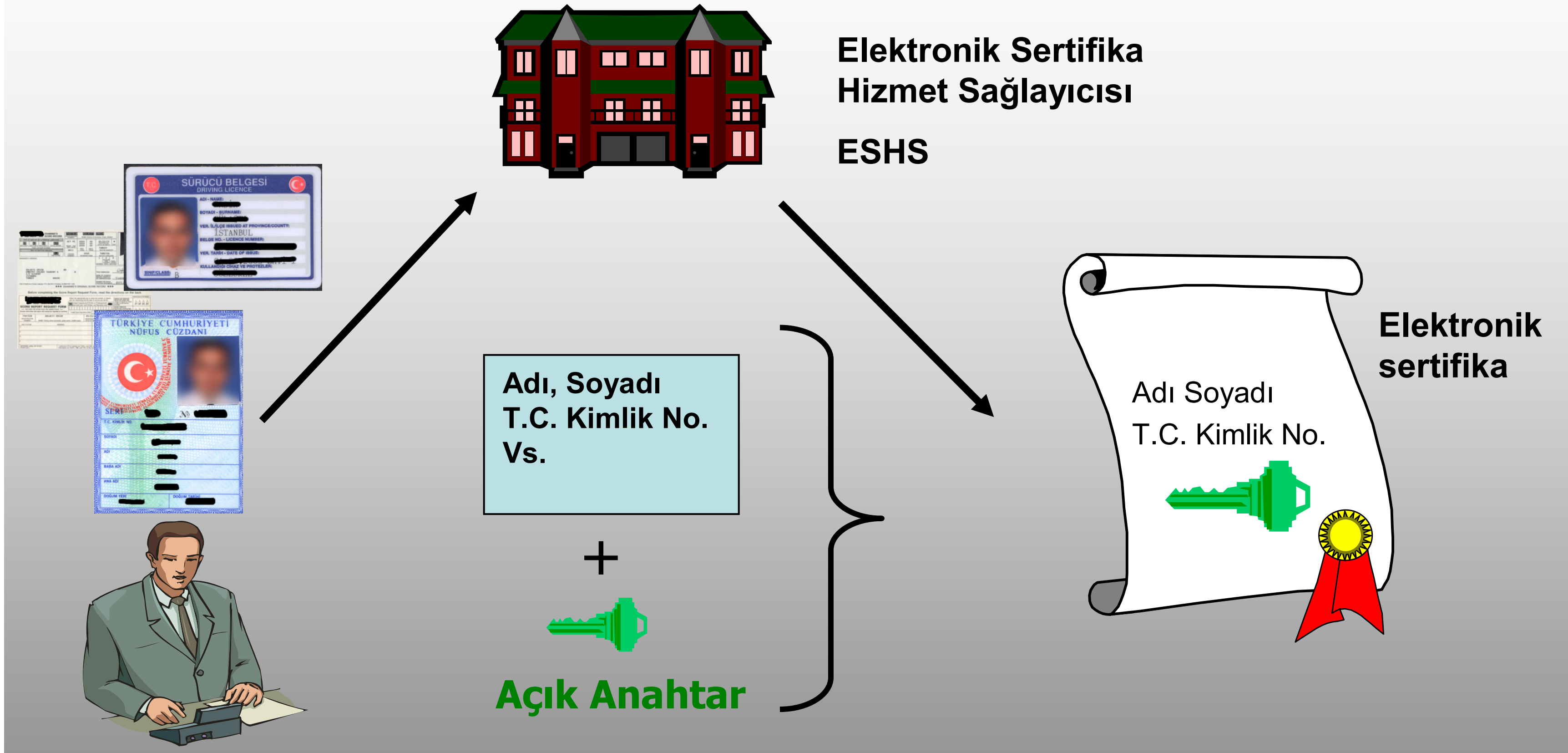
Elektronik imza, imzanın atıldığı belgenin içeriği de kullanılarak oluşturulur.

Kullanılan Teknoloji

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

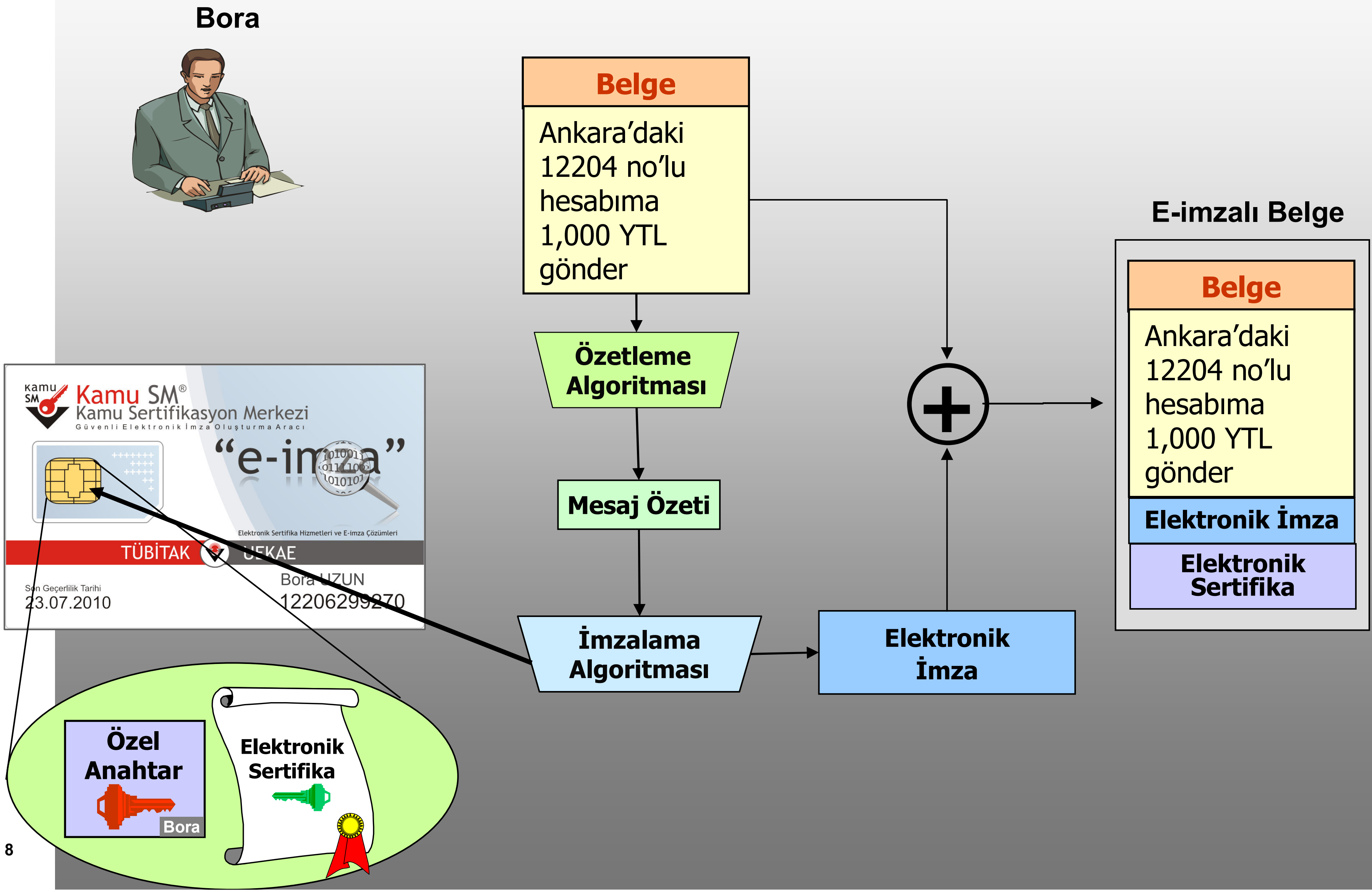


Elektronik Sertifika: İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kayıttır

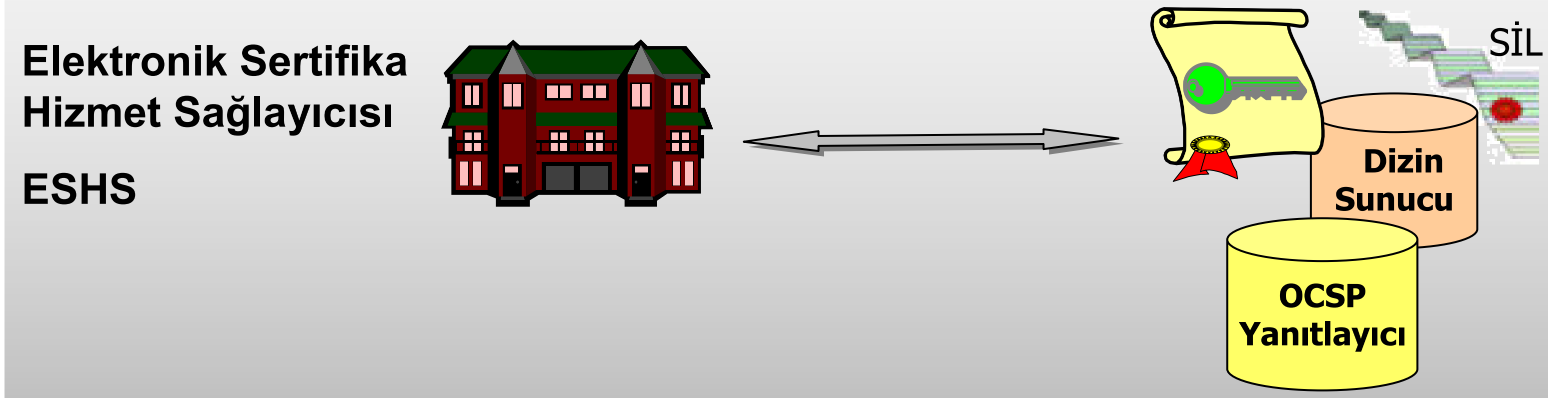
E-imzalı Belge Oluşturma

TASNİF DIŞI

Elektronik İmzalı Bir Belge Nasıl Oluşturulur?



Elektronik Sertifikanın Doğrulanması



- 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

Türkiye'de E-imza

- 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 Sertifika Kullanımı

Nitelikli Elektronik Sertifika Kullanımı

Kurum Adı	Toplam
ADALET BAKANLIĞI	6.643
TÜBİTAK	1.174
TCDD	1.164
DEVLET SU ISLERI	779
BANKACILIK DÜZENLEME VE DENETLEME KURUMU	505
TELEKOMÜNIKASYON KURUMU BASKANLIGI	483
GÜMRÜK MÜSTESARLIGI	461
DIŞ TİCARET MÜSTEŞARLIĞI	375
TÜRKİYE PETROLLERİ A.O.	300
TÜRKIYE ISTATISTIK KURUMU	290
TÜRKIYE 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 ILÇE MILLI EGITIM MÜDÜRLÜGÜ	63
İSKİ	60
SANAYI VE TICARET BAKANLIGI	50

İmzager Yazılımı

Güvenilir imza doğrulama işlemlerinde referans olarak kullanılacak bir araç sunmak.

www.kamusm.gov.tr

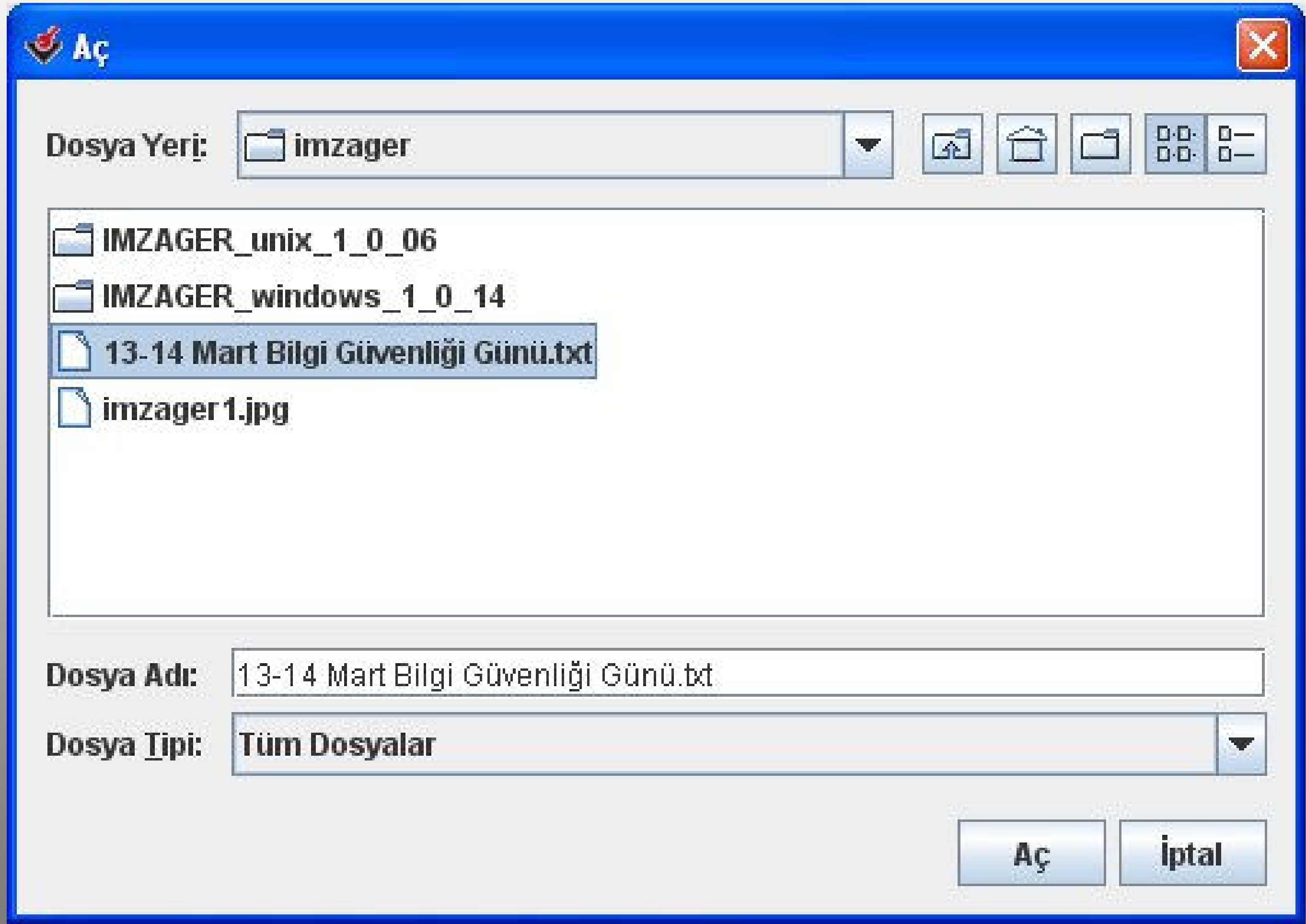
İmzager Yazılımı Özellikleri

TASNİF DIŞI

- 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

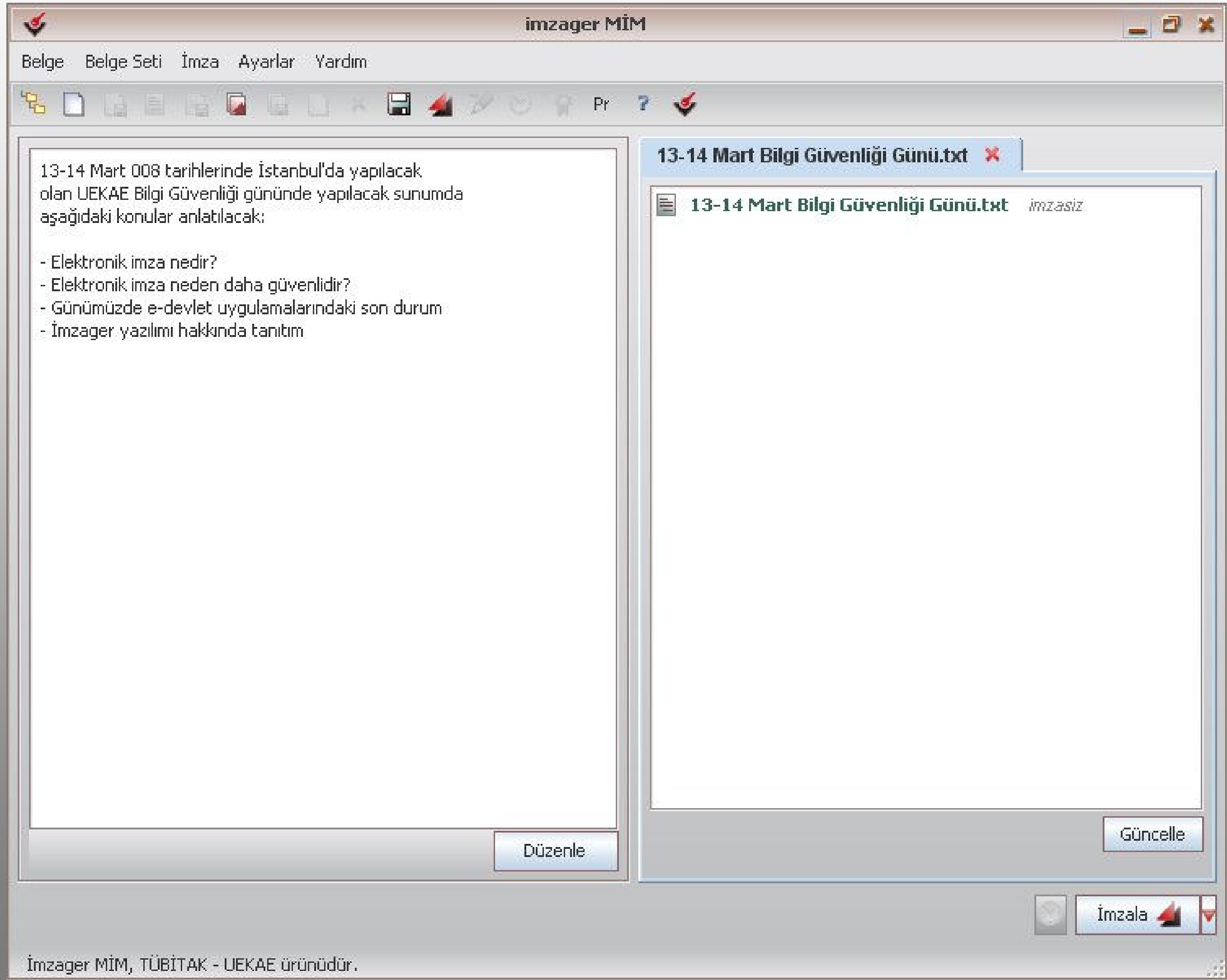
İmzager Kullanımı

Bir dosya seçelim

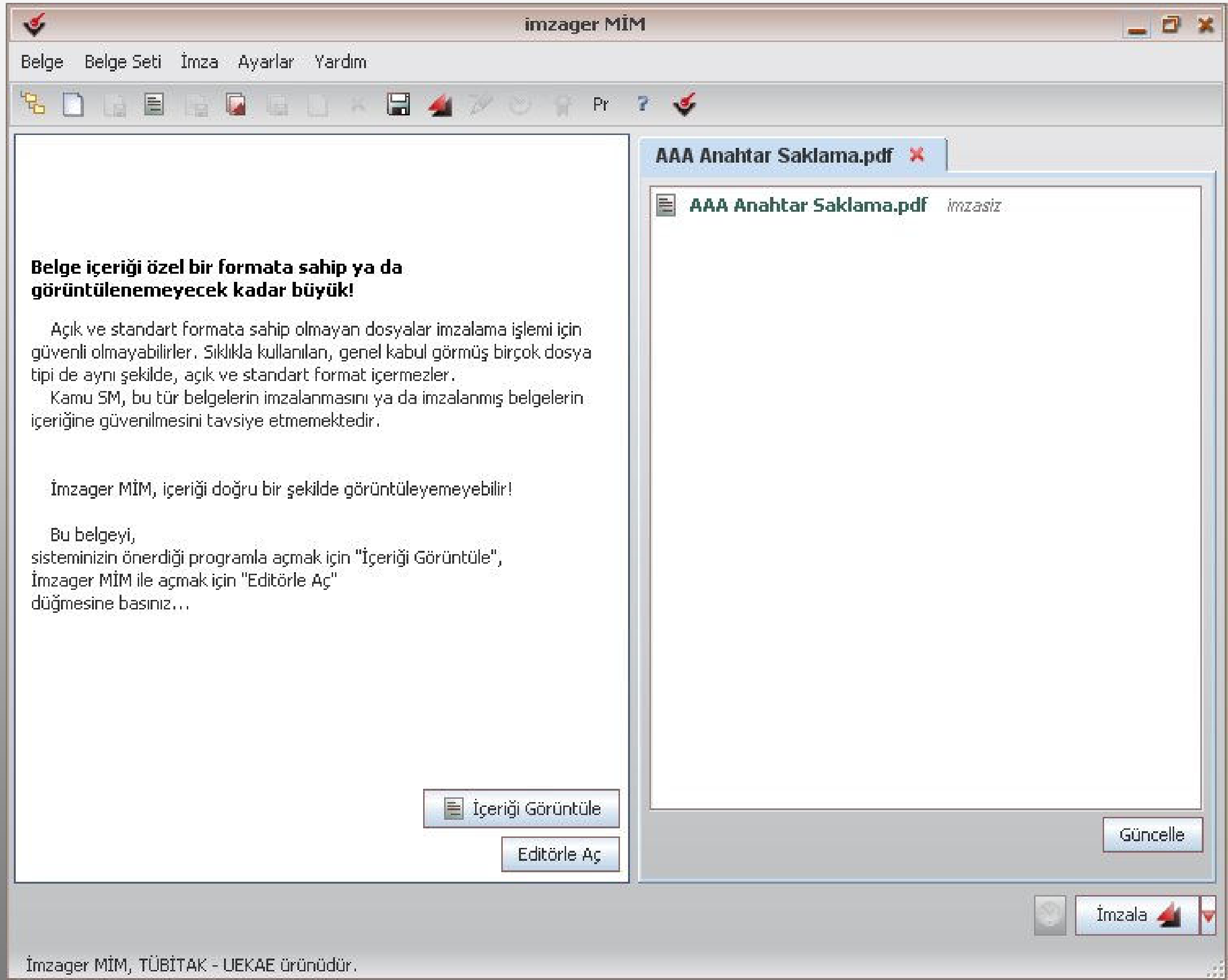


İmzager Kullanımı

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

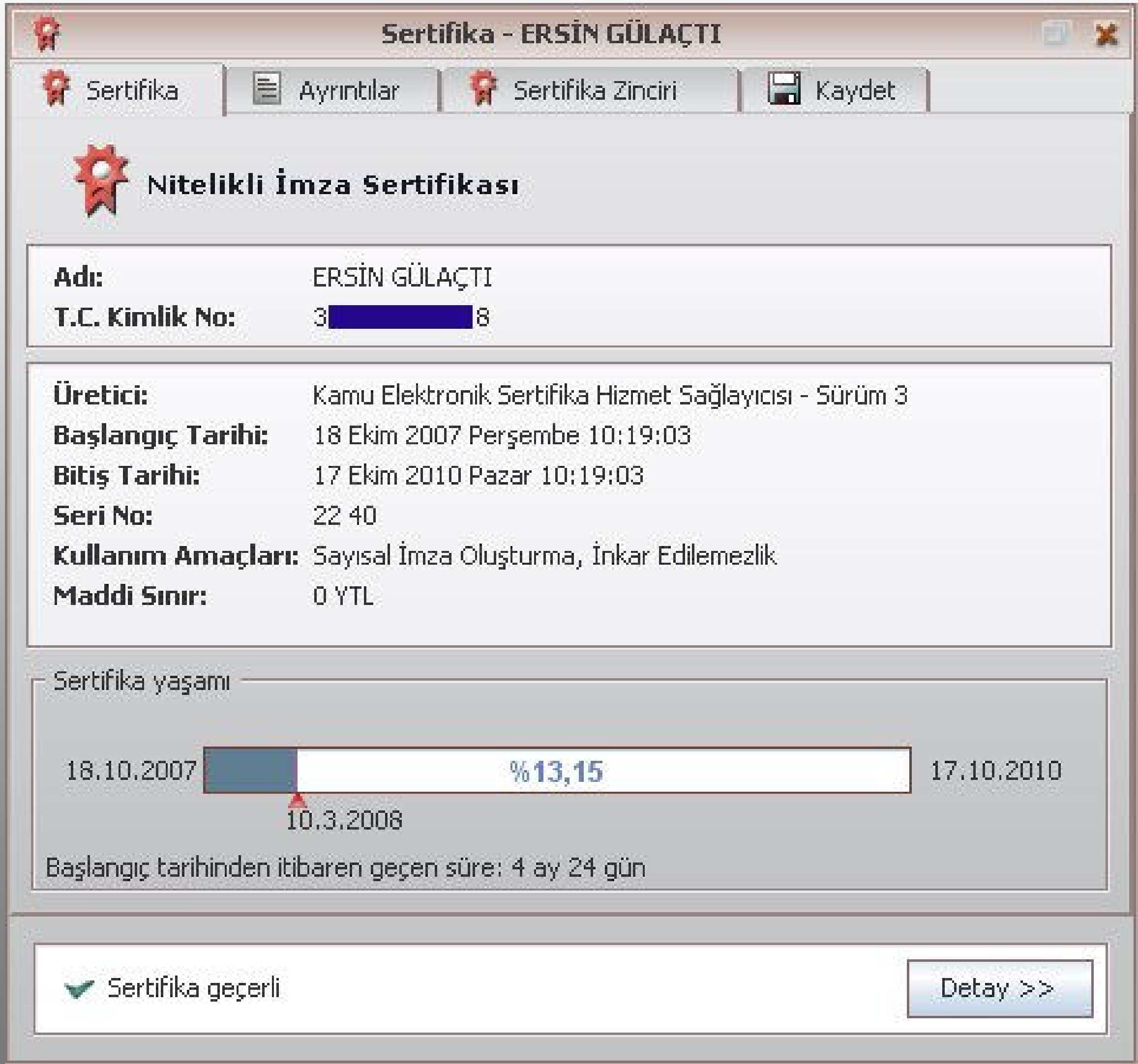


Bilinmeyen içerik için uyarı verilir



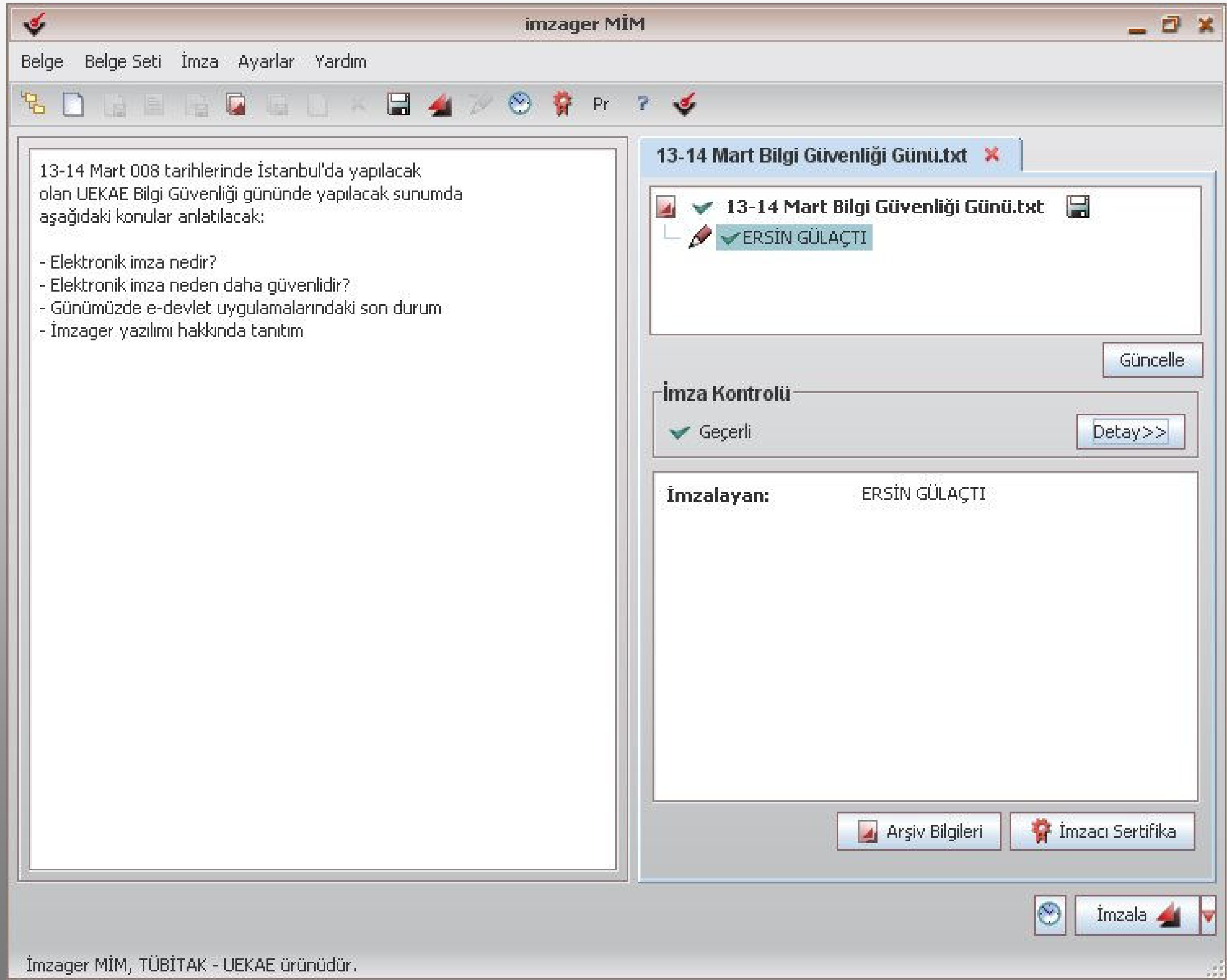
Akıllı kart parola giriş ekranı açılır

İstenirse sertifika görüntülenir



İmzager Kullanımı

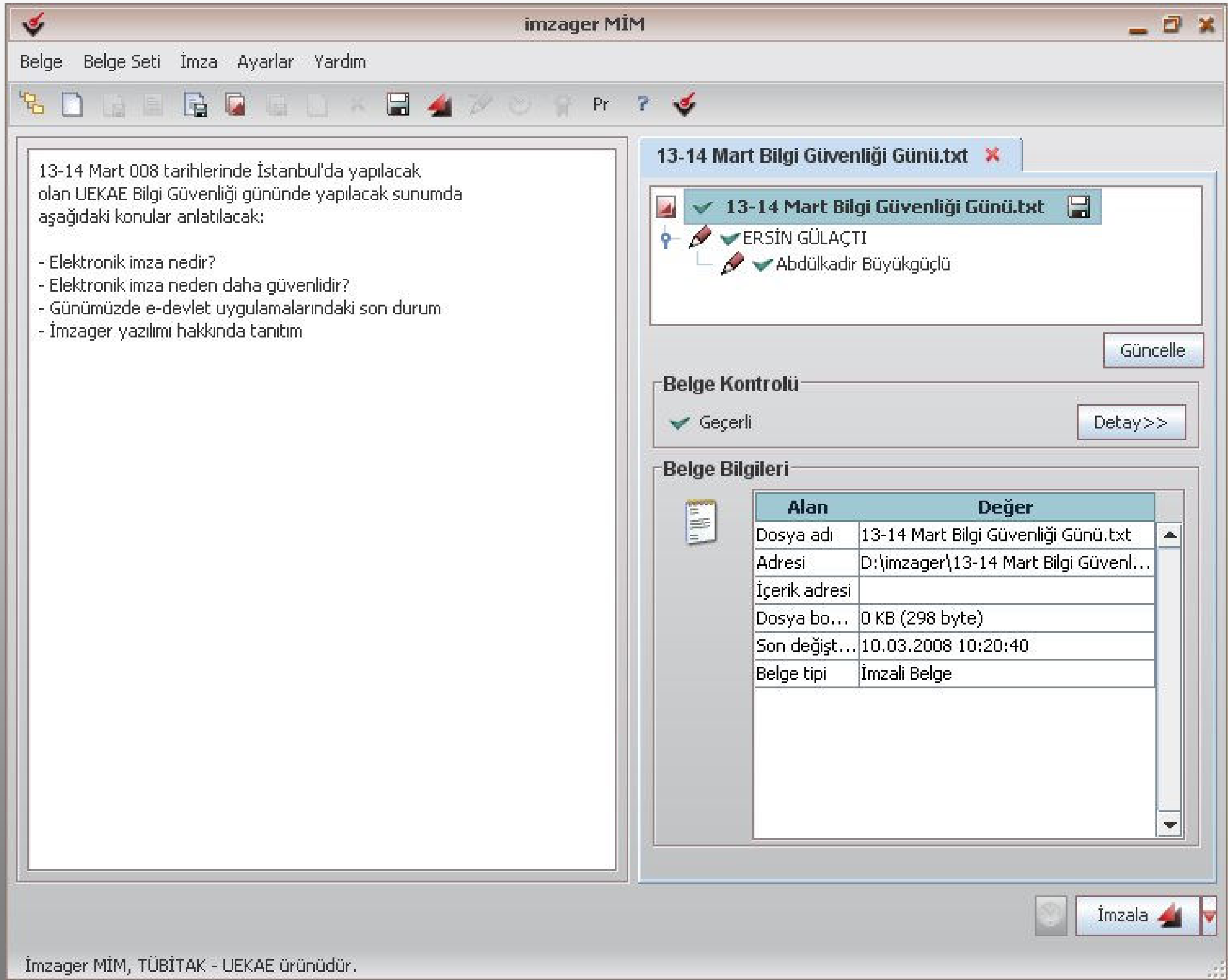
İmza oluşturulur ve “imz” uzantılı olarak kaydedilir



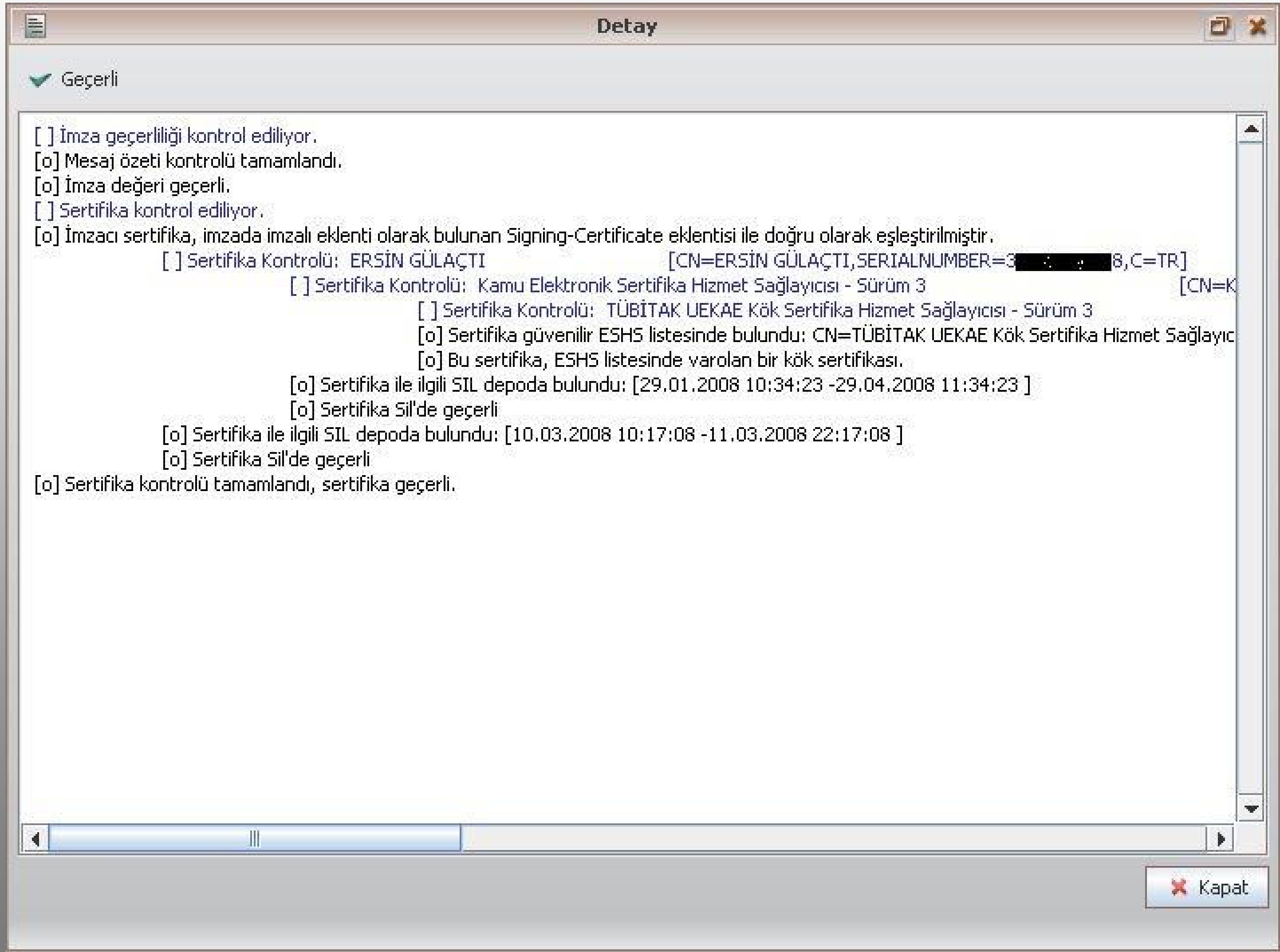
İmzager Kullanımı

TASNİF DIŞI

Çoklu imzalar atılabilir



İmzanın kontrolü ile ilgili detaylı bilgi alınabilir



Sorular