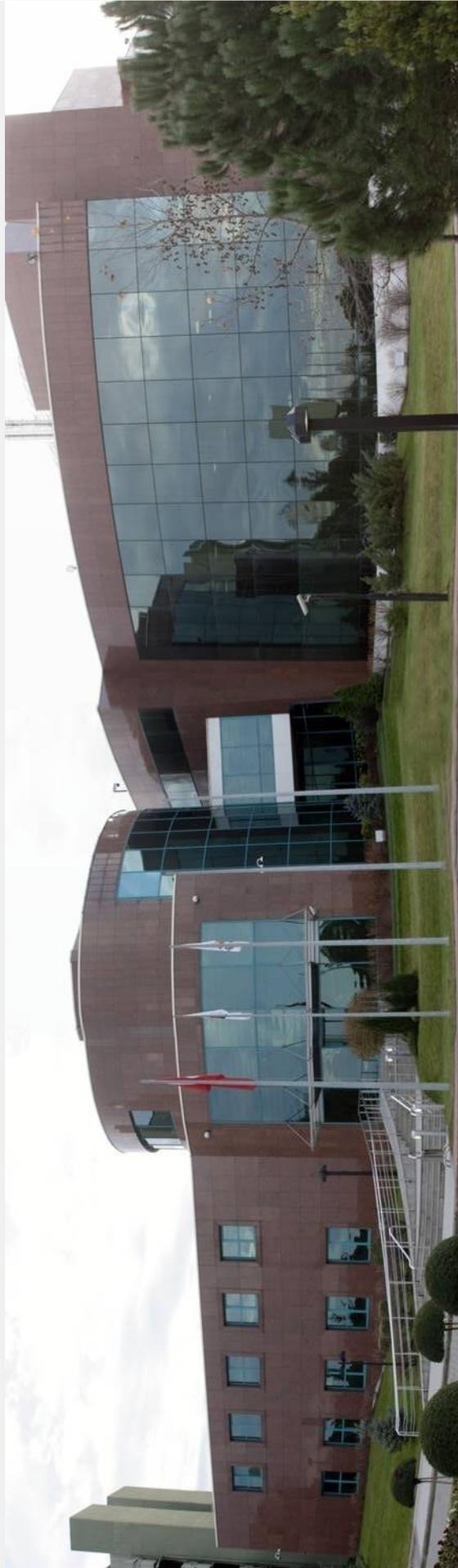




TÜBİTAK  
**UEKAE**



## Elektronik İmza ve Güvenlik

Ersin GÜLACHTI

Kamu Sertifikasyon Merkezi Yöneticisi

Mart, 2008

TASNİF DİŞİ



## Konular

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



## **Elektronik İmza Nedir?**



TASNİF DİŞİ

## **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 Sağlıar?

- Bilgi bütünlüğü
- Kimlik doğrulama
- İnkar edilemezlik

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

# Elektronik İmzanın Islak İmzadan Farkı

TASNIF DIŞI



İslak imza  
Örnekleri

Dilekçe

—  
—  
—  
—

Eser

Çek

—  
—  
—  
—

Eser

Senet

—  
—  
—  
—

Eser

Elektronik imza  
Örnekleri

E-Fatura

—  
—  
—  
—

C044E5...9665

E-Dilekçe

—  
—  
—  
—

AB02FA...0374

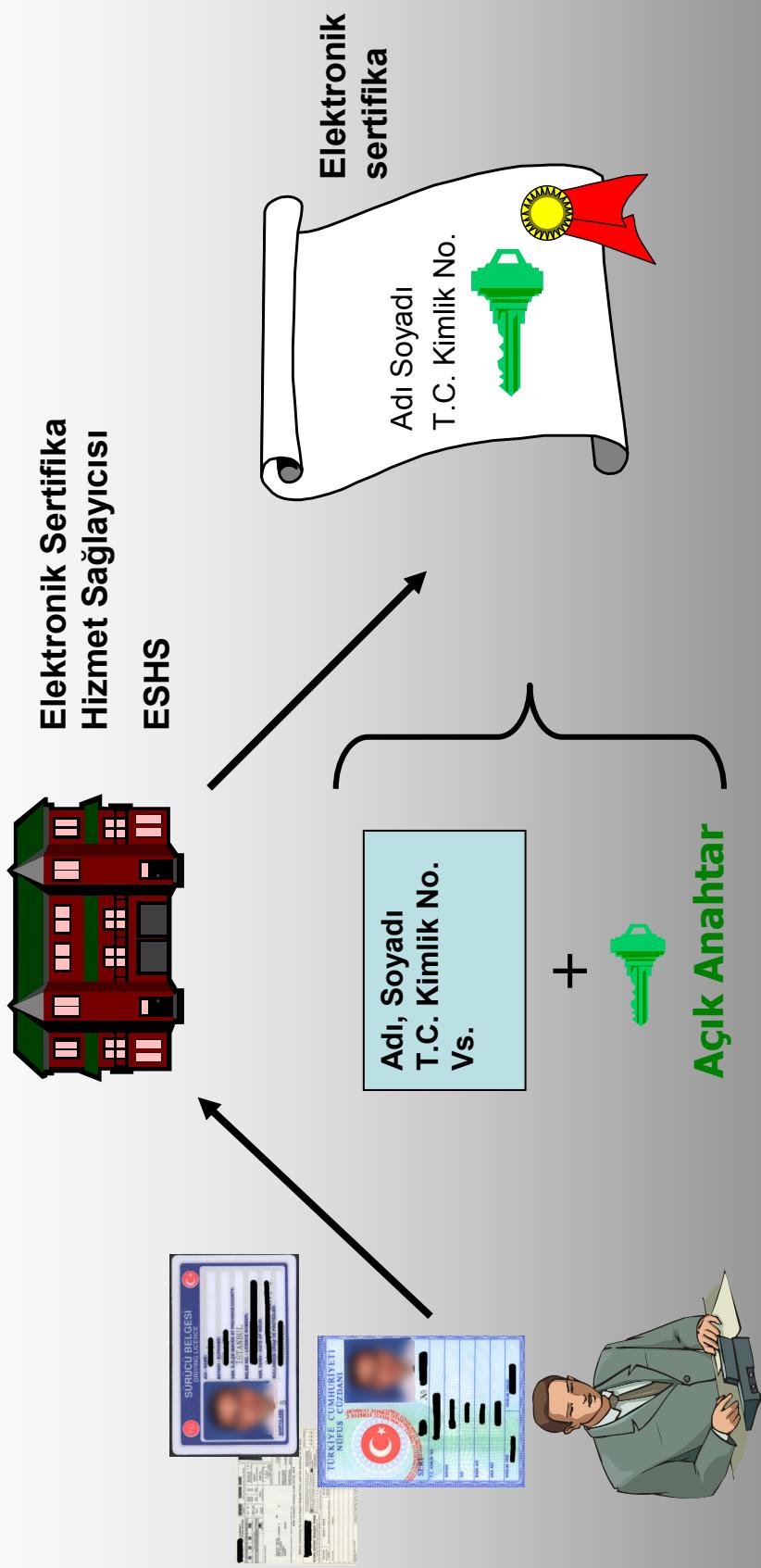
**Elektronik imza, imzanın atıldığı belgenin içeriği de  
kullanılarak oluşturulur.**

## 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..)
- Özeti algoritması kullanılır (SHA, RIPEM, vs..)

# Elektronik Sertifikalar

TASNIF DIŞI



**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



<b>Belge</b>
Ankara'daki 12204 no'lu hesabına 1,000 YTL gönder

### E-imzalı Belge

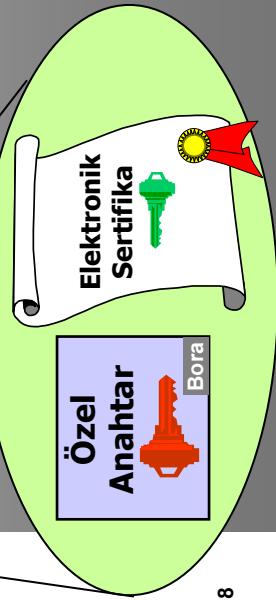
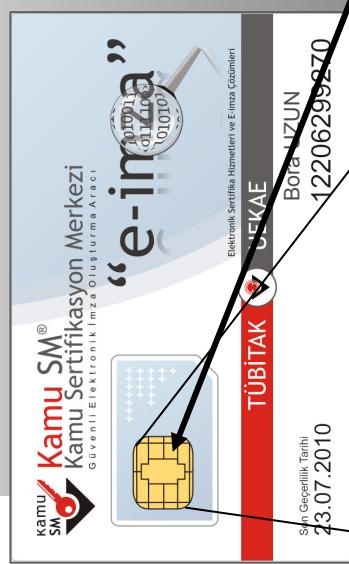
<b>Belge</b>
Ankara'daki 12204 no'lu hesabına 1,000 YTL gönder
<b>Elektronik İmza</b>
<b>Elektronik Sertifika</b>

### Özetleme Algoritması

### Mesaj Özeti

### İmzalama Algoritması

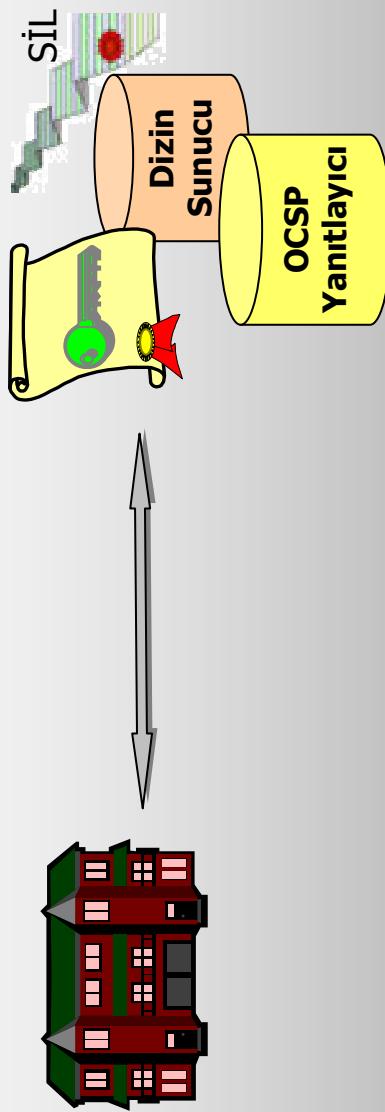
### Elektronik İmza



## Elektronik Sertifikanın Doğrulanması

TASNIF DIŞI

**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?



TASNIF DIŞI

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

## Türkiye'de E-imza



TASNIF DIŞI

- 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



TASNIF DIŞI

**80** Nitelikli Elektronik Sertifika talepleri üzerine  
uygulama analizi gerçekleştirilen kurum  
sayısı

**52** İmza yazılım kütüphanelerinin kullanımına  
sunulduğu kurum ve kuruluş sayısı

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

Verilmiş olan nitelikli elektronik sertifika  
sayısı  
**14,000**

# Nitelikli Sertifika Kullanimı

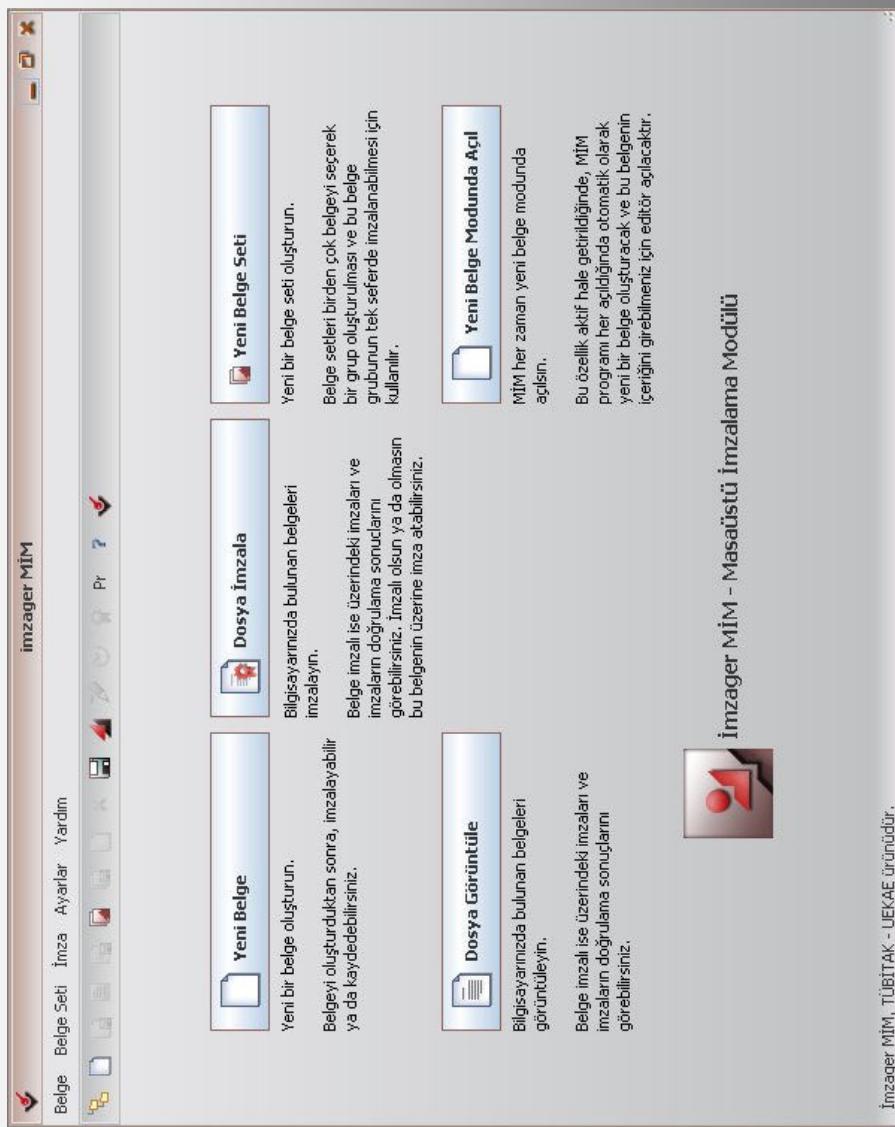


TASNIF DIŞI

# Nitelikli Elektronik Sertifika Kullanimı

Kurum Adı	Toplam
ADALET BAKANLIĞI	<b>6.643</b>
TÜBİTAK	1.174
TCDD	1.164
DEVLET SU İSLERİ	779
BANKACILIK DÜZENLEME VE DENETLEME KURUMU	505
TELEKOMÜNIKASYON KURUMU BASKANLIĞI	483
GÜMRÜK MÜSTEREŞARLIĞI	461
DIŞ TİCARET MÜSTEREŞARLIĞI	<b>375</b>
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 MÜSTEREŞARLIĞI - SERBEST BÖLGELER	216
DEVLET MALZEME OFİSİ GENEL MÜDÜRLÜĞÜ	186
MALİYE BAKANLIĞI MASAK	136
T.C. KOCAELİ BÜYÜKŞEHİR BELEDİYE BAŞKANLIĞI	103
BAKIRKÖY İLÇE MILLİ EĞİTİM MÜDÜRLÜĞÜ	63
İŞKİ	60
SANAYİ VE TİCARET BAKANLIĞI	<b>50</b>

## Güvenilir imza doğrulama işlemlerinde referans olarak kullanılacak bir araç sunmak.



İmzager MİM, TÜBİTAK - UEKAE ürünüdür.

**www.kamusum.gov.tr**

## İmzager Yazılımı Özellikleri

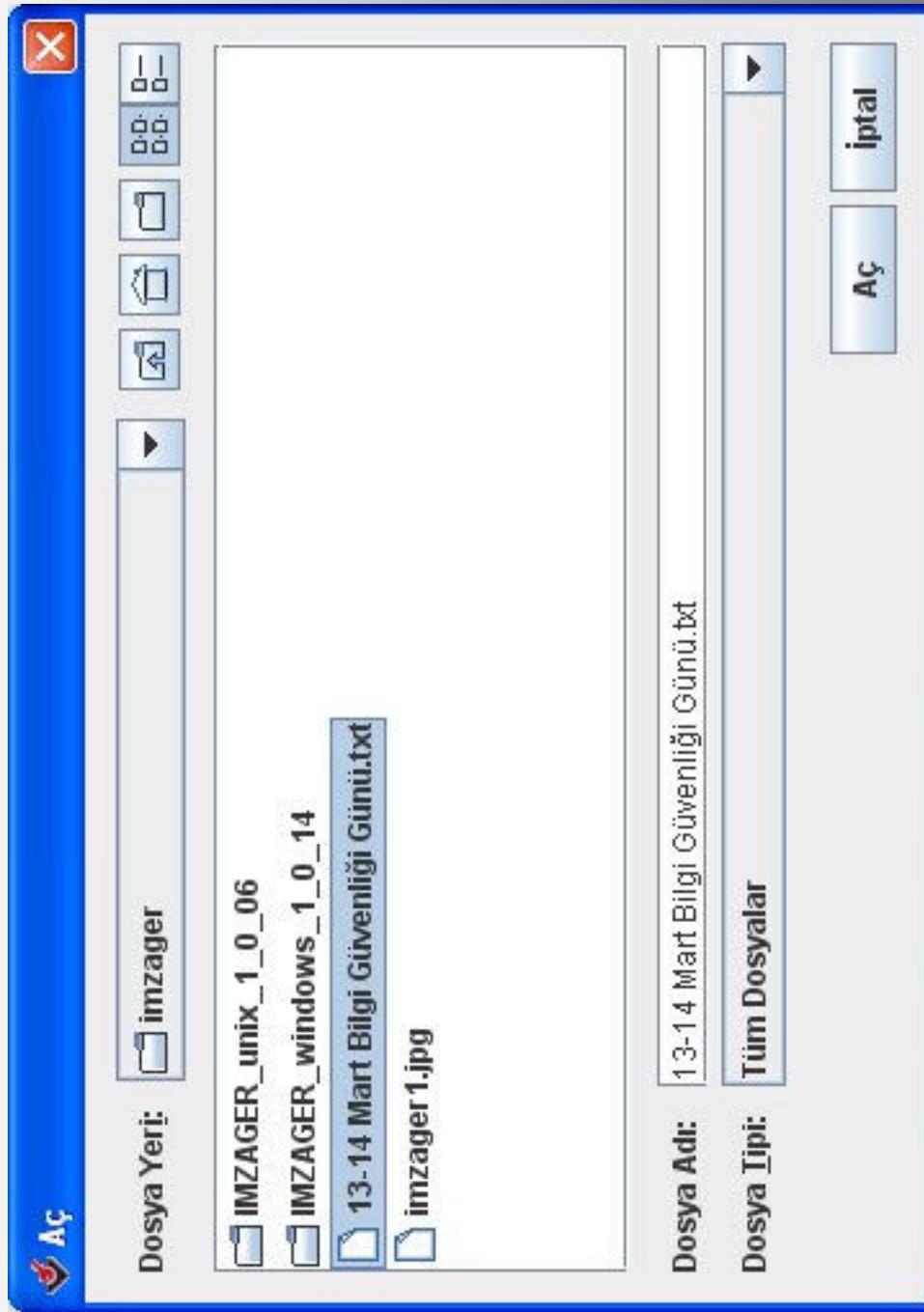
- ETSI 101733 standartına uyumlu
  - Seri imza atma
  - Zaman damgası alma
  - Basit, gelişmiş, arşiv imzası doğrulama
  - Seri-paralel imza doğrulama
- Java tabanlı, platform bağımsız
- KamuSM sertifikaları ile imza atma, tüm nitelikli imzaları doğrulama

# İmzager Kullanımı



TASNİF DİŞİ

## Bir dosya seçelim

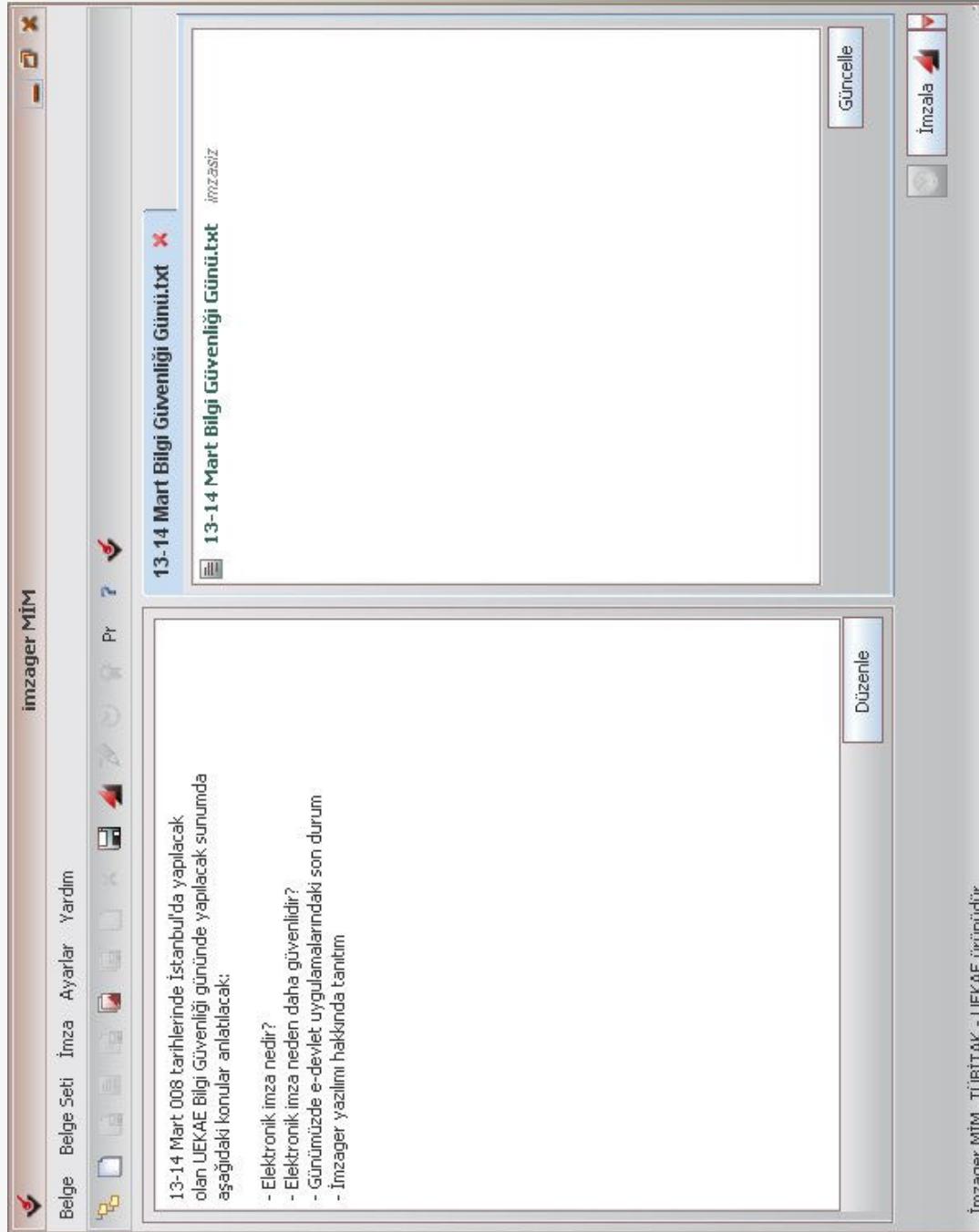


# İmzager Kullanımı



TASNIF DIŞI

## Bilinen bir içerik (txt, zmf, jpg, tif, gif) görüntülenenir



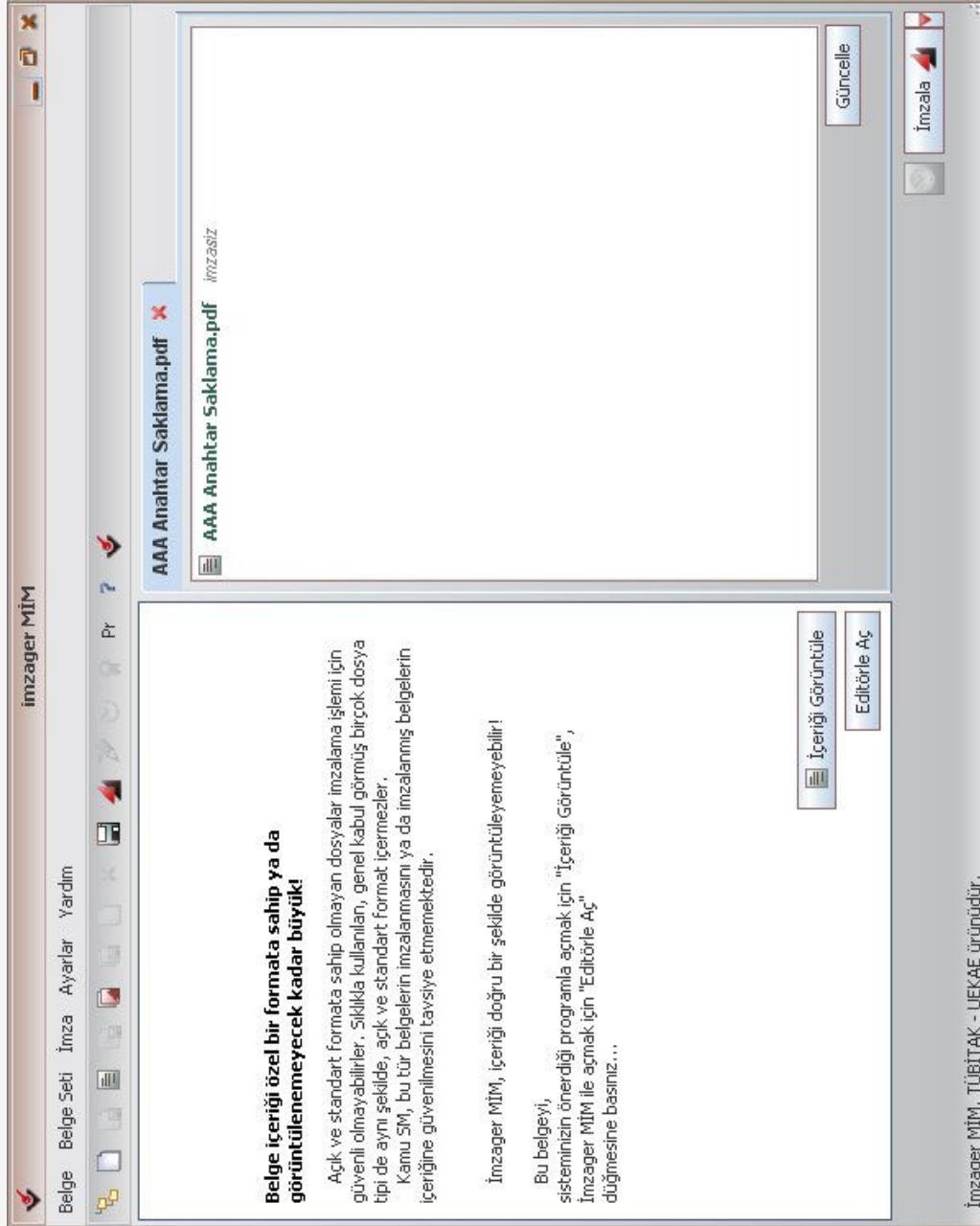
İmzager MIM, TÜBITAK - UEKAE ürünüdür.

# İmzager Kullanımı



TASNIF DIŞI

## Bilinmeyen içerik için uyarı verilir



İmzager MIM, TÜBİTAK - UEKAE ürünüdür.

# İmzager Kullanımı



TASNİF DİŞİ

## Akıllı kart parola giriş ekranı açılır

PIN Giriş

Seçili Sertifika

ERSİN GÜLAÇTİ

Görüntüle

Seç

Akıllı kart PIN kodunu giriniz...

\* \* \* \* \*

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

Rakamları karıştır

Tamam

İptal

# İmzager Kullanımı



TASNIF DİŞİ

## İstenirse sertifika görüntülenenir

Sertifika - ERŞİN GÜLAÇTI

Sertifika Ayrıntılar Sertifika Zinciri Kaydet

Nitelikli İmza Sertifikası

Adı: ERŞİN GÜLAÇTI  
T.C. Kimlik No: 3 ██████████ 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, İnkar Edilemezlik  
Maddi Sınır: 0 YTL

Sertifika yaşımlı

18.10.2007 %13,15 17.10.2010  
10.3.2008 Başlangıç tarihinden itibaren geçen süre: 4 ay 24 gün

Sertifika geçerli

Düzenle >>

# İmzager Kullanımı



TASNIF DIŞI

## İmza oluşturulur ve “imz” uzantılı olarak kaydedilir

imzager MİM

Belge Belge Seti İmza Ayarlar Yardım

13-14 Mart Bilgi Güvenliği Günü.txt

13-14 Mart Bilgi Güvenliği Günü.txt

13-14 Mart Bilgi Güvenliği Günü.txt

ERSİN GÜLAÇTI

Güncelle

Düzenle >

İmza Kontrolü

Geçerli

İmzalayan: ERSİN GÜLAÇTİ

Arşiv Bilgileri İmzacı Sertifikası

İmzala

İmzager MİM, TÜBİTAK - UEKAE ürünüdür.

# İmzager Kullanımı



TASNIF DIŞI

## Çoklu imzalar atılabilir

The screenshot shows the Imzager MIM application interface. At the top, there's a toolbar with various icons for file operations like Open, Save, Print, and Sign. The main window has a title bar "imzager MIM". Below the toolbar, there's a menu bar with "Belge", "Belge Seti", "İmza", "Ayarlar", and "Yardım".  
  
The central area displays a document titled "13-14 Mart Bilgi Güvenliği Günü.txt". A status bar at the bottom of this window indicates "13-14 Mart Bilgi Güvenliği Günü.txt" and shows icons for "ERSİN GÜLAÇTI", "Abdulkadir Büyüğücü", and "Geçerli".  
  
On the right side of the application, there are two panels:

- Belge Kontrolü:** Contains a "Güncelle" button and a "Düzenle" button.
- Belge Bilgileri:** A table with columns "Alan" and "Değer". It lists the following information:

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

  
In the bottom right corner of the application window, there's a "İmzala" button with a red arrow icon.

İmzager MIM, TÜBİTAK - UEKAE ürünüdür.

# İmzager Kullanımı



TASNIF DIŞI

## İmzanın kontrolü ile ilgili detaylı bilgi alınabilir

Detay

▼ Geçerli

[ ] İmza geçerliliği kontrol ediliyor.  
[o] Mesaj özeti kontrolü tamamlandı.  
[o] İmza değeri geçerli.  
[ ] Sertifika kontrol ediliyor.

[o] İmzacı sertifika, imzada imzalı ekleni olarak bulunan Signing-Certificate eklientisi ile doğru olarak eşleştirilmişdir.  
[CN=ERSİN GÜLACHTI,SERIALNUMBER=3... : ..., 8, C=TR]  
[ ] Sertifika Kontrolü: ERSİN GÜLACHTI  
[ ] Sertifika Kontrolü: Kamu Elektronik Sertifika Hizmet Sağlayıcı - Sürüm 3  
[ ] Sertifika Kontrolü: TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3  
[o] Sertifika güvenilir ESHS listesinde bulundu: CN=TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcı  
[o] Bu sertifika, ESHS listesinde varolan bir kök sertifikası.  
[o] Sertifika ile ilgili SIL depoda bulundu: [29.01.2008 10:34:23 -29.04.2008 11:34:23 ]  
[o] Sertifika SIL'de geçerli  
[o] Sertifika ile ilgili SIL depoda bulundu: [10.03.2008 10:17:08 -11.03.2008 22:17:08 ]  
[o] Sertifika SIL'de geçerli  
[o] Sertifika kontrolü tamamlandı, sertifika geçerli.

➤ Kapat

## Sorular

TASNİF DİŞİ

