



TÜBİTAK UEKAE

ULUSAL ELEKTRONİK ve KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ

TASNİF DIŞI

E-İmza ve Kamu Sertifikasyon Merkezi



Mustafa C. Kuşçu

Tel: 0 262 648 1871

e-Posta: mck@uekae.tubitak.gov.tr
mustafa.kuscu@kamusm.gov.tr

Ocak 2006



Kamu Sertifikasyon Merkezi

TASNİF DIŞI

- e-Dönüşüm Türkiye İcra Kurulu Kararı (10 Haziran 2004)
- Başbakanlık Genelgesi (6 Eylül 2004)
- Kamu SM: TÜBİTAK UEKAE
- Koordinasyon:
Telekomünikasyon Kurumu & DPT



Görev ve Hedeflerimiz

- Kamu Sertifikasyon Yapısı'nın oluşturulması
 - Kök Sertifika Hizmet Sağlayıcısı
 - Kamu Sertifika Hizmet Sağlayıcısı
- Kamu kurum ve kuruluşlarının kurum içi ve kurumlar arası işlemlerde kullanacakları nitelikli elektronik sertifika ihtiyaçlarının tek merkezden karşılanması
- Dileyen Elektronik Sertifika Hizmet Sağlayıcılarına kök sertifika hizmeti sağlanması



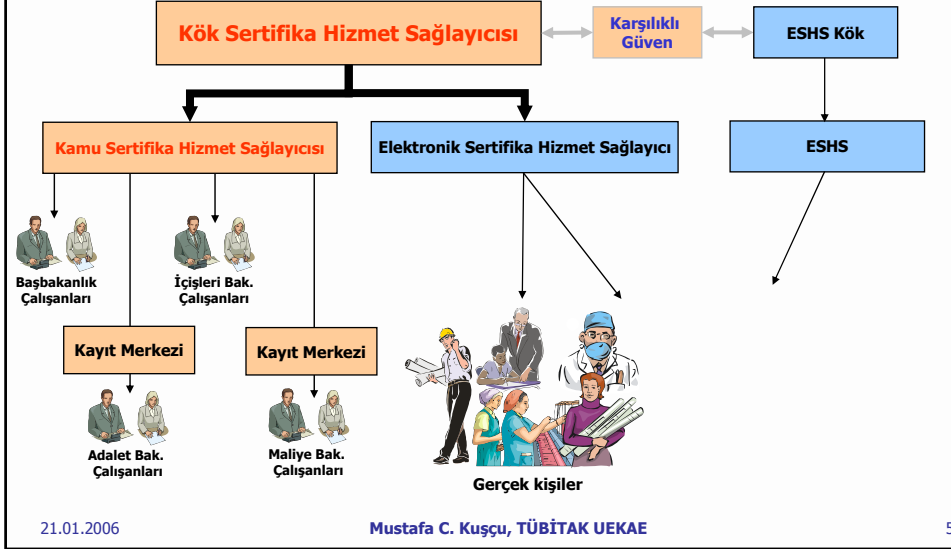
Görev ve Hedeflerimiz

- Elektronik imza konusunda toplumsal bilinç oluşmasına katkıda bulunmak
- Elektronik imza teknolojisinde milli katkı oranını yükseltmek
- ESHS olmak isteyen kuruluşlara yazılım desteği vermek, operasyonel deneyimleri aktarmak



Elektronik Sertifika Yapısı

TASNİF DIŐI



Elektronik İmza ve e-Devlet

TASNİF DIŐI

Kontrol Listesi:

1. Teknolojik altyapısı hazır mı?
2. İş süreçleri uygun mu?
3. e-Devlet için önemi yüksek mi?
4. Niyetli mi?

21.01.2006

Mustafa C. Kuşçu, TÜBİTAK UEKAE

6



Elektronik İmza ve e-Devlet

Sürec:

1. Sistem mühendisliđi
 2. Uygulama uyarlama
 3. Test
 4. Sertifika hazırlama & dağıtma
 5. Devreye alma
- Yazılım sağlama (*API, lib, ...*)
 - Eğitim
 - Danışmanlık
 - Çözüm sağlama



Kamu Kurumları ve E-imza

- Başvuran kamu personeli sayısı > 1000
- Kısa vade talep sayısı
100 000 – 150 000
- 2006 hedefi
30 000
- 2005 Temmuz-Aralık gerçekleşen
450



TASNİF DIŐI

Sertifika Hizmetleri

- Nitelikli Elektronik Sertifika
 - 3 yıl sertifika geçerlilik süresi – 99 YTL/sertifika
 - Dizin servisinde ücretsiz yayınlama
 - Ücretsiz sertifika iptal durum kaydı hizmetleri
 - Çevrimiçi Sertifika Durum Protokolü (OCSP) hizmeti ile çevrimiçi sertifikaların geçerlilik kontrolü
 - Sertifika İptal Listesi hizmeti
- Sertifika yaşam döngüsü hizmetleri
 - Sertifika iptal taleplerinin alınması
 - Geçerlilik süresi sonunda sertifika yenileme
 - Sertifika bilgilerinin güncellenmesi

21.01.2006

Mustafa C. Kuşçu, TÜBİTAK UEKAE

9



TASNİF DIŐI

Diğer Ürün ve Hizmetlerimiz

- İmza E-imza yazılım kütüphanesi, API, Applet ürünleri ve desteği
- İmzager Masaüstü İmzalama Yazılımı
- Akıllı Kart Yönetim Yazılımı

21.01.2006

Mustafa C. Kuşçu, TÜBİTAK UEKAE

10



- ETSI (Avrupa Birliđi) elektronik imza formatı
 - Farklı imza tipleri
 - İmzalanan belgenin türüne, kullanım amaçlarına göre, deđişik ihtiyaçları karşılayacak imzalama tipleri
 - Temel imza
 - Zaman damgalı imza
 - İlkeli imza
 - Arşiv imzası
- İmza bilgileri
 - Yetki bilgisi
 - Yer bilgisi
 - İmza amacı
 - Referans belge numarası
 - Belge format bilgisi
 - Zaman damgası



- Sertifikalar -opsiyonel olarak eklenip çıkarılabilir-
- XML ve ASN.1 standardı
- Java ve .net desteđi
- Seri/paralel imza ekleme
- İmzalı belgeden imza çıkarma
- Zaman damgası kontrolü
- OCSP ve SİL kontrolü



E-imza Web Appleti

TASNİF DIŐI



- Kanuna uygun olarak “Nitelikli Elektronik İmza” atabilir
- Üzerinde “Kamu SM”nin imzasını taşır
- Web tabanlı sistemlerde, kullanıcıların yaptıkları imzalama işleminin tamamen KamuSM e-imza programları tarafından gerçekleştirildiğini garanti eder
- Web sitesi sahibi, yöneticisi, ya da programcısına ait tüm hata, güvenlik eksikliği ya da yanlış yönlendirmeleri, ayrıca kötü niyetli saldırıları, korsan faaliyetleri engeller

21.01.2006

Mustafa C. Kuşçu, TÜBİTAK UEKAE

13



E-imza Web Appleti

TASNİF DIŐI



- Kanuna uygun olarak “Nitelikli İmza” atabilme
 - Mevzuata uygun bir şekilde imza içeriğini göstererek imza atılmasını sağlar
- Çoklu kart okuyucu ve çoklu sertifika desteği
- İmza kontrolü yapabilme
- İmza ve sertifika bilgilerini gösterebilme

21.01.2006

Mustafa C. Kuşçu, TÜBİTAK UEKAE

14



TASNİF DIŐI

Masaüstü Dosya İmzalama



- İmzagerAPI'nin sahip olduđu özellikleri kullanabilme
- Her tip dosya imzalayabilme
 - Standart ve açık olmayan formatlara sahip dokümanların içeriđi tam olarak garantilenemediđi için, bu dokümanların imzalanması KamuSM tarafından tavsiye **edilmemektedir**.
 - İmzalama işlemindeki tüm sorumluluk kullanıcıya aittir.

21.01.2006

Mustafa C. Kuşçu, TÜBİTAK UEKAE

15



TASNİF DIŐI

Akıllı Kart Yönetim Yazılımı



- Kart okuyucu bilgileri
- Kart bilgileri gösterimi
- Sertifika işlemleri (silme, ekleme, çıkarma)
- PIN, PUK deđiştirebilme
- Güvenilir ESHS sertifikaları ile çalışabilme

21.01.2006

Mustafa C. Kuşçu, TÜBİTAK UEKAE

16



İletişim Bilgileri

TASNİF DIŐI

Her türlü soru, görüş ve
önerileriniz için:

Kamu Sertifikasyon Merkezi

Çağrı Merkezi: (262) 648 18 18

Faks: (262) 648 18 00

bilgi@kamusm.gov.tr

Sunan:

Mustafa C. Kuşçu

(262) 648 18 71

mustafa.kuscu@kamusm.gov.tr