



Türkiye'de E-İmza

Emre Yüce

Portakal Teknoloji

emre.yuce@portakalteknoloji.com

2. Özgür Yazılım Konferansı

Ankara, 20 Haziran 2008



Sunum Planı

- Elektronik imza nedir?
 - Kriptografik altyapı
 - Simetrik şifreleme
 - Asimetrik şifreleme
 - E-imza uygulaması
 - Açık anahtar altyapısı
- Türkiye'de e-imza
 - Düzenlemeler
 - ESHS'lar
 - Kullanım alanları
- Mobil Elektronik İmza (mobil e-imza)
 - Dünya'da mobil e-imza



portakal

Elektronik imza nedir?

- Kimlik dođrulama (authentication)
- Bütünlük (integrity)
- İnkâr edememe (non-repudiation)



Kriptografik altyapı

- Simetrik şifreleme (DES, Rijndael vs.)
- Asimetrik şifreleme (RSA, El-Gamal)



Simetrik şifreleme

- Tek anahtar
 - Anahtar dağıtım problemi
- Hızlı şifreleme ve deşifre etme



Asimetrik şifreleme

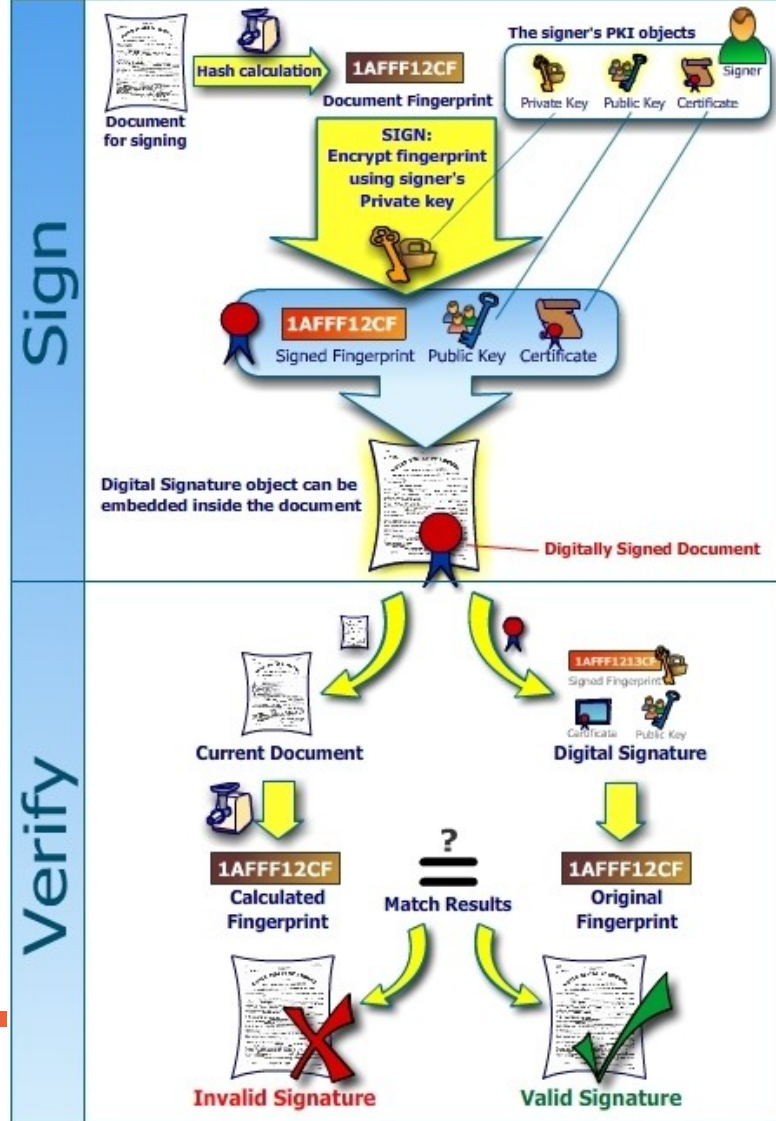
- Açık (public) ve özel (private) olmak üzere 2 anahtar.
 - Açık anahtarın duyurulması, Güvenilir üçüncü kişi (trusted third party)
- Yavaş şifreleme ve çözme
- Açık anahtarın bilinmesi özel anahtar hakkında bilgi vermiyor.
- Simetrik anahtar değişimi için ideal.



Asimetrik şifreleme kullanımı

- Şifreleme:
 - Kişinin açık anahtarını kullanarak herkes mesaj gönderebilir.
 - Sadece doğru kişi özel anahtarını kullanarak mesajı açabilir.
- İmza:
 - Kişi özel anahtarı ile mesajı şifreler (imzalar)
 - Kişinin açık anahtarını kullanarak herkes mesajı doğrulayabilir.

Elektronik imza uygulaması



- Mesajın özet değeri hesaplanır.
- Kişi özel anahtarı ile bu özeti imzalar.
- Bu imzayı mesaja ekler ve karşı tarafa yollar.
- Karşı taraf imzayı onaylar.
- Kimlik doğrulama, bütünlük ve inkar edilemezlik özellikleri sağlanır.
- Gizlilik için ayrıca şifreleme gereklidir.

Elektronik imza uygulaması

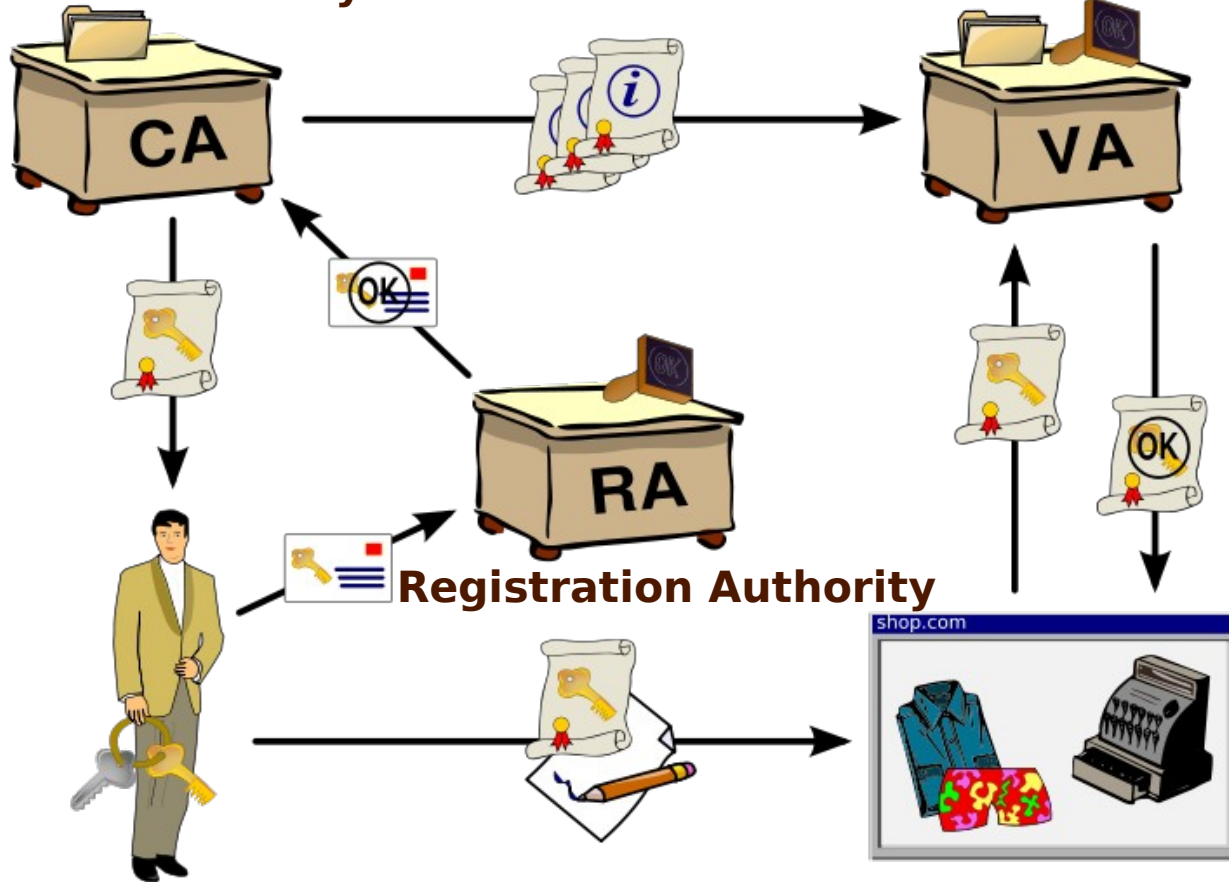
- Kart okuyucular
- USB token
- Biometrik bilgi
- Şifre ile koruma



Açık anahtar altyapısı

Certificate Authority

Verification Authority





Türkiye'deki e-imza düzenlemeleri

- 5070 sayılı Elektronik İmza Kanunu (23 Ocak 2004 tarih ve 25355 sayılı Resmi Gazete)
- Sertifika Mali Sorumluluk Sigortası Yönetmeliği (26 Ağustos 2004 tarih ve 25565 sayılı Resmi Gazete)
- ...

*Daha fazla bilgi için: <http://www.tk.gov.tr/Tuketici/Sorularlar/Sorularlar.htm>



Elektronik sertifika hizmet sağlayıcısı

- Açık anahtar altyapısını oluşturur.
- Nitelikli sertifika dağıtma yetkisine sahiptir.
- Kullanıcılar için sertifika yayımlar.
- Sertifika durum bilgilerini güncel tutar ve sertifika iptal listeleri hazırlar.
- Güncel sertifikaları ve sertifika iptal listelerini isteyen kişilere sunar.
- Süresi dolan ya da iptal edilen sertifikaların arşivini tutar.



Türkiye'deki ESHS'ler

- Elektronik Bilgi Güvenliği A.Ş. (E-Güven) 24.06.2005
- TÜBİTAK-UEKAE (Kamu Sertifikasyon Merkezi) 30.06.2005
- TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş. 16.07.2005
- EBG Bilişim Teknolojileri ve Hizmetleri A.Ş.(E-Tugra) 01.09.2006

**Bu bilgiler <http://www.tk.gov.tr/eimza/eshs.htm> adresinden alınmıştır.*



Muhtemel e-imza kullanım alanları

- Kamusal Alandaki Uygulamalar
 - Her türlü başvurular (ÖSS, KPSS, LES, pasaport vb)
 - Kurumlararası iletişim (Emniyet Müdürlükleri, Nüfus ve Vatandaşlık İşleri Müdürlükleri vb)
 - Sosyal güvenlik uygulamaları
 - Sağlık uygulamaları (Sağlık personeli - hastaneler - eczaneler)
 - Vergi ödemeleri
 - Elektronik oy verme işlemleri



Muhtemel e-imza kullanım alanları

- Ticari Alandaki Uygulamalar
 - İnternet bankacılığı
 - Sigortacılık işlemleri
 - Kağıtsız ofisler
 - E-Sözleşmeler
 - E-Sipariş



Mobil Elektronik İmza

- Akıllı kart olarak sim kart.
- Açık anahtar altyapısına gsm operatörü de dahil.
- Özel anahtar sim kartta saklanıyor. İmzalama işlemi simkartta yapılabilir. (veya güvenli imza sunucusunda yapılıyor.)
- Uygulamaları
 - Bankalarda
 - Adalet Bakanlığı UYAP projesinde.
 - Sanayi Bakanlığı'nda
 - Gümrük başvurusunda
 - Aile hekimliği sisteminde kullanılıyor.



Dünyada Mobil e-imza

- Finlandiya'da vatandaşlık ve adres bilgilerini değiştirmekte askerlik, e-fatura, marka, patent ve çalışma bakanlığı işlemlerinde;
- Estonya'da park ücretlerini ödemede;
- Norveç'te mobil ticarete, bankacılık işlemlerinde;
- Fransa'da otopark ücretlerini ödemede, at yarışında, oyun makinalarında (yaş onaylaması için) veya telefonla dondurma siparişi vermekte kullanılabiliyormuş

Teşekkürler, Sorularınız ve Görüşleriniz

Sunuma ulaşabileceğiniz adresler:

<http://www.emreyuce.com>

<http://www.portakalteknoloji.com>

<http://blogs.portakalteknoloji.com/emre>

Kaynak: Telekomünikasyon Kurumu: <http://www.tk.gov.tr/>