



Gerçek Yaşamda;
AAA Riskleri
Türkiye'de E - imza

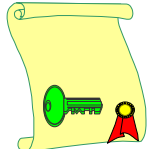
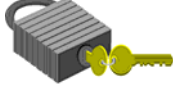
Abdullah Battal, Gülay Yalçın, Ruken Zilan

TOBB Ekonomi Teknoloji Üniversitesi

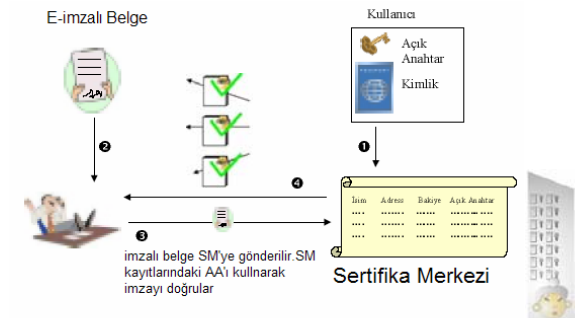
Ana Başlıklarla Kapsam

- Açık Anahtar Altyapısı
- AAA'daki Riskler ve Uygulama Zorlukları
 - Güncel Yaşamda Karşılaşılan Riskler
 - Başlıca Uygulama Zorlukları
- Türkiye'de Bankacılık ve E-ticaret Uygulamaları
 - Bankacılık Uygulamaları & Sorunları
 - E-Ticaret
- Türkiye'de E-imza Karşısında Duran Sorunlar
- Öneriler ve Sonsöz

AAA (Açık Anahtar Altyapısı)



SM Kullanarak E-İmzalı Belge Doğrulama



E-İmzalı Belge

Kullanıcı

Açık Anahtar Kimlik

İmza Adresi E-posta Açık Anahtar

Sertifika Merkezi

İmzalı belge SM'ye gönderilir. SM kayıtlarındaki AA'ı kullanarak imzayı doğrular

SM kullanarak e-İmzalı belge doğrulama

AAA'daki Riskler ve Uygulama Zorlukları

Güncel Yaşamda Karşılaşılan Riskler

- Anahtar Yönetimine Bağlı Riskler
- Risk Oluşturan Sistemsel Hatalar
- Risk Oluşturan Kullanıcı Hataları

Anahtar Yönetimine Bağlı Riskler

- Sertifikaların son kullanım tarihleri, güncellenme süreleri, imhaları ve **bu süre içinde kırılabilme ihtimalleri.**
- Web üzerinden yayınlanan sertifika iptal listelerine **kötü niyetlilerce ulaşılması ihtimali.**

Risk Oluşturan Sistemsel Hatalar

- Sertifikanın kişiye/kuruma teslim şekli.
 - > Floppy disk, email vb.
- Korunmayan bir sertifikanın ele geçirilmesi.
 - > Virüs,trojan vb.
- Sertifika Merkezinin gizli anahtarının ele geçirilmesi.
 - > Sertifika Sağlayıcıların kullandığı "kök" açık anahtar listesine bir başkasının kendi anahtarını ekleyerek, **kendi sertifikasını başka bir sertifikanın yerine göstermesi.**
- Sertifikaların sadece isim ile ilişkilendirilmesi sonucunda isimler arası karışıklıklar oluşması.

Risk Oluşturan Kullanıcı Hataları

- Özel anahtarların çalınması problemi
 - Trojan, virüs.
- Kişilerin özel anahtarını kaybetmesi.
 - Gönderilmiş olan şifrelenmiş metinlerin ulaşamaz hale gelebilir.

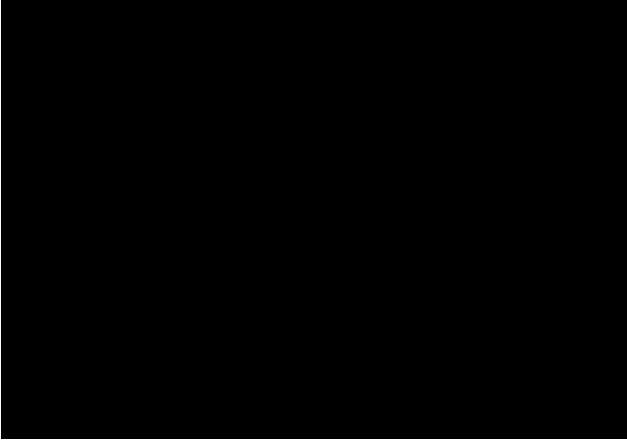
Başlıca Uygulama Zorlukları

- Kişisel Gizliliğin Korunamaması
 - Alınan sertifikalar ile kişisel bilgilerin internette dolaşımı.
- İptal Edilen Sertifikalarla İlgili Sorunlar ve Riskler
 - SM günde birkaç kere SİL yayınlar.
- Kayıtlardaki Zorluk ve Riskler
 - Online kayıtlar.
- Güven Sorunu
 - "Sertifika güvenli olsaydı tarayıcı ile gelirdi"
- Sertifikalarda Bir Standart Yakalanamaması
 - X509 v3, ancak SM eklentileri farklı.
- Hız Sorunu
 - AAA sebebi ile yavaş.

Türkiye'de Bankacılık ve E-ticaret Uygulamaları

Bankacılık Uygulamaları ve Sorunları

- Kullanıcı Bilgilerinin Ele Geçirilmesi
 - Trojan, Key-Logger, Screen Logger
- Site ve Web Sayfası Sahteciliği
 - Banka sitesine benzer siteler, sahte kilit işareti, benzer isimli sertifikalar.
- Kimlik Doğrulama ve İnkâr Edilemezlik
 - Tek yönlü kimlik doğrulama.
- Kullanıcı Bilgilerine Yönelik Saldırımlar
 - Deneme Yanılma, Telefon Bankacılığı
- Teknolojik Gelişmelerin Takip Edilmemesi
 - MD5 kullanımı



Türkiye'de AAA ve Bankacılık

- Türkiye bankaların AAA uygulamalarında ciddi güvenlik sorunları bulunmaktadır:
 - Önlemler **standartlaşmaya yönelik değildir**.
 - Ethereal programı ile paketlerin incelenmesi sonucunda, işlemlerin yapıldığı bilgisayarın **SHA algoritmasını desteklemesine rağmen**, sunucunun **MD5 hash algoritmasını** seçtiği görülmüştür.
 - **Müşterilerin** de açık anahtar altyapısı sistemine **dahil edilmeleri** gerekir.

E-ticaret

- AAA sayesinde kimlik kartı bilgileri ağ üzerinde **güvenli** bir şekilde **ilettilip** kontrol edilmektedir (SSL ve SET).
- Kredi kartının başkası tarafından kullanılmasını **engellememektedir**.
- **Yeterli deneme** sonucunda geçerli kredi kartı bilgileri **bulunabilir**.

Türkiye'de E-imza Karşısındaki Sorunlar

E-imza Karşısındaki Sorunlar

- Yasa Kapsamında Suiistimale Müsait Maddeler
- Teknolojiden Kaynaklı Uygulama Güçlükleri
- Uyumluluk Sorunları
- Bilgi ve Bilinç Eksikliği
- Yüksek Uygulama Maliyetleri

Yasa Kapsamında Suiistimale Müsait Maddeler

- İmzanın nerelerde kullanılmayacağı net olarak ifade edilmemiş olması (Madde5).
- Sertifika iptal işlemlerinin kurumlara bırakılıp, hiçbir standart belirtilmemiş olması.
- Kamu kurumlarının denetim ve cezadan muafiyeti (Madde 21).
- İmza sahibi kanunda tanımlanmış olsa da imza sahibinin sorumluluklarına kanunda yer verilmemiş olması.

Yasa Kapsamında Suiistimale Müsait Maddeler

- Yasada sertifikaların uluslararası kullanımı için bir standart olmaması.
- Sertifikadaki alanların standartlaşmamış olması ve her bir alanın farklı şekilde düzenlenebilmesi.
- E-Belge ile ilgili hiçbir hukuki düzenlemenin yapılmamış olması.
 - Belgelerin asıllarının sunulma zorunluluğu karşısında elektronik verilerin çıktılarının durumu.

Yasa Kapsamında Suiistimale Müsait Maddeler

- Zaman Damgası'nın Kanunda yalnızca bir tanım olarak bulunması (Madde 3).
- İmza atma ve doğrulama araçları olan Applet ve Api'lerin adının yasada geçmemesi.
 - Usul ve esaslarda ise imza atma ve doğrulama araçlarının temini kriterlere bağlanmadığından, istenilen yerden alınabilecek durumdadır.

Yüksek Uygulama Maliyetleri

- **Dijital imza teknolojilerinin** yüksek maliyetli uygulamalar olması.
- Sertifika kullanıcılarının, **kart, okuyucu ve token gibi yazılım ve donanım** gereksinimlerinin yanı sıra, **sertifikalara** da belli bir ücret ödemek durumunda olması.
- Sertifikadan, sertifika sahibine veya diğer kişilere doğabilecek zararlar için **mali sorumluluk sigortası** yaptırma zorunluluğu.

Öneriler



- **Genel Öneriler**
- **Bankacılıkla İlgili Öneriler**
- **E-İmza ile İlgili Öneriler**

Genel Öneriler

- Sistemi güvenlik konularında bilgisiz kullanıcılar dahi **kolay ve güvenli** şekilde kullanabilmelidir.
- Hız sorunu olabildiğince ortadan kaldırılmalıdır.
- Kart okuyucusu olarak PIN kodu üzerinden girilen **portatif okuyucular** tercih edilmelidir.
- **Sertifika iptalleri** için ucuz ama **belirsiz süreyi en aza indirecek** bir metodun geliştirilmesi zaruridir.
- **Sertifika İptal Listelerine**, olası riskler göz önüne alınarak, herkes tarafından **ulaşım** sağlanmalıdır.

Bankacılıkla İlgili Öneriler

- Bankacılık işlemlerinde güvenliği sağlamak konusunda **standartlaşma** yapılmalıdır.
- Bankalarda **NES** kullanımının olmaması sebebi ile online bankacılık işlemlerinin **yasal hükmü bulunmamaktadır**. Bankalarda NES kullanımı yaygınlaştırılmalıdır.
- Müşteriler de, **e-imza ve sertifika** kullanımına geçmelidir.
- Günümüz teknolojisi ile değerlendirildiğinde SHA-512 veya daha **güvenli bir hash algoritmasının** kullanımına geçilmelidir.
- Bankaların anlaşılmalı olduğu ve **dünyaca tanınan Sertifika Merkezlerinin attığı imzaların** Türkiye'de de **tanınması** için gerekli hukuksal altyapı hazırlanmalıdır.

E-imza Kanunu İle İlgili Öneriler

- E imzaya tabi olmayacak **istisnai durumlar** tek tek ifade edilmelidir.
- Sertifikalara global çapta bir standartlaşma getirilmesi gerekmektedir.
 - Sertifikalarda **alanların** standart olması gerekmektedir.
 - “**Api ve applet’lerde** bir standarda varılmalıdır. Ve üretimleri yetkililere verilmelidir.
 - **Sertifika iptal işlemi** tüm kurumlar için belli bir standartla belirtilmelidir.
 - Yoruma açık **zaman damgası kavramının** da standartları ifade edilmelidir.

E-imza Kanunu İle İlgili Öneriler

- Yasada sadece imza olarak kullanılabileceği ifade edilen **e-imzanın kimlik doğrulama sorununa çözüm** getirilmelidir.
- Kamu kurumlarının denetim ve cezalardan **muaf tutulmasını** öneren maddeye **yeni bir düzenleme** getirilmelidir.
- Yasalarda gerekli hukuksal ayarlamalar yapılmalıdır:
 - E-imzanın belge çıktısı üzerinden tespit edilemeyeceği gerçeğinin yasalarda göz önüne alınması.
 - Mahkemelerin e-imza altyapısına hazır hale getirilmesi.
 - Kanunlarda bulunan “belgelerin asıllarının sunulma zorunluluğu” kavramının e-belgenin durumu göz önüne alınarak düzenlenmesi.

Son Söz

- **Açık Anahtar Altyapısı, son yıllarda bilgisayar güvenliği alanında çok tartışılan konulardan biri olmuştur. Ancak uygulama alanındaki sorunlar üzerinde durulmaması sebebi ile sadece teorik olarak değerini korumaktadır.**
- Bu çalışma sonucunda, günümüzde e-imzanın güvenli şekilde uygulanabilmesi için birçok **tedbir alınması gerekliliği görülmüştür.**
- **Uygulama güçlükleri getiren; teknolojik, bireysel, uyumsal ve maddi sorunların bir an önce giderilmesi veya en aza indirgenmesi gerekmektedir.**
- Yasal düzenlemelerin asla ihmal edilmemesi ve bu yasal düzenlemeler yapılmadan e-imzanın yaygınlaştırılmaması gerektiği sonucuna varılmıştır.

TEŞEKKÜRLER

