

Internet'te Hekim (Hasta) Tanılaması ve Veri Güvenliği

Sağlık Bilişimi Oturumlar
Inet-tr'03 Konferansı
12 Aralık, Cuma
İstanbul

Mete Varas,
varas@tursign.com



Gerçek İhtiyaçlar Gerçek Talep

- Rekabet
- Yasa koyucu, düzenleyici ve bağımsız kurumların sık talepleri.
- Müteeriler ile olan anlaşmazlık ve açılan dava sayısının giderek artması.
 - Karşı ortamlarda “yasal amaçlı kanıt bulmanın” çok büyük maliyetleri olması.
- Kar marjlarının giderek küçülmesi.
 - Her karşı ortamına dönüş insan, zaman ve süreç maliyeti getirir
 - Karşıtlar saklamak çok büyük maliyet
 - Karşıtlar göndermek çok büyük maliyet
- İnternetin yaygın olarak kullanılması nedeniyle müteeri beklentilerini arttırması.
 - Karşı ortamlarda kalmak kısa/orta/uzun dönemde müteeriyi kaybetmek demektir.

Yasal Geli meler

- Amerika Birle ik Devletleri E- mza Yasas (2000)
- Avrupa Birli i E- mza Direktifi (1999-2002)
- Arjantin, ili, Hindistan, dahil bir çok lke e-imza yasalar
- HIPPA (Health Insurance Portability and Accounting Act 1996)
- FDA-21 (The Federal Drug Administration) CFR 11 and 203 (2000)

HIPPA

- ▣ Sağlık kurumlarının gizli sağlık bilgilerinin gizliliğini, güvenliğini ve standartların korunması için elektronik sistemlerde belli normlara uyulmasını artırmaktadır.
- ▣ Tüm hasta kayıtları (veritabanları, sağlık sigortası başvuruları dahil) ve tüm sağlık kurumları (hastaneler, sağlık ocağı dahil)
- ▣ Bilgiyi alan kişilerin alması gereken durumu nedir?
- ▣ Tutulan veriler izinsiz erişimlere karşı korunuyor mu?
- ▣ Taraflar görmeleri gereken bilgileri görmüyorlar mı?
- ▣ Taraflar –aldıkları bilgileri- daha sonra almadıkları için inkar edebiliyorlar mı?

FDA-21 CFR 11 & 203

- Kayıt ve imza gereksinimlerinde kağıt ortam ve slak imza yanında elektronik imzanın kullanılmasına da izin vermiştir.
- İlaç, biyoteknoloji ve tıp cihazları şirketleri (FDA onaylı kurumlar)
- Zorunlu olmamasına rağmen de i im çok hızlı olmaktadır.

Hedef

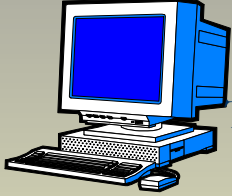
Geli en “yeni nesil e-i uygulamalar n” desteklemesi için yeni tan lama ve eri im kontrolü çözümleri geli tirmek..

- ▣ Milyonlarca say da kullan c için,
- ▣ Kolay kurulum ve yönetimi olan,
- ▣ Kullan c lar için daha kolay ve kapsaml
- ▣ Birden çok platformda kullan m (Internet, VPN, mobil)

Tanlamada Karşılaşılan Problemler



Çalınlar



Tedarikçiler



Ortaklar



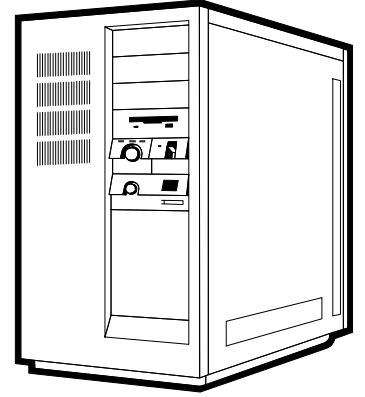
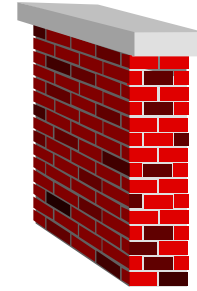
Müşteriler

Internet

VPN

SSL

Fire Wall



Web Site
Sunucusu

TURSign

Tan lama Yöntemleri

Yüksek

G
Ü
V
E
N
L
K

Zayıf

Düşük

+ Yüksek Seviyeli Tan lama

+ Tanımlanabilirlik

- Kaybolma ve Kırılma

- Unutma

- Yüksek Maliyetler

- Dijital Mızalama Atamama

□ Kripto Ak ll Kartlar

□ Ak ll Kartlar

□ Hardware Tokenlar

+ Yüksek Seviyeli Tan lama

+ Dijital Mızalama

- Kaybolma ve Kırılma Olas l

- Tanımlanabilir De il (okuyucu)

- Yüksek Maliyetler

+ Geni Uygulama Alan

+ Kullan c Dostu ve Al lım

- Dijital Mızalama Atamama

- Kolayl kla De i tirilir

□ Kullan c Ad

+ ifre

KULLANIM

(son kullan c ve servis sunucusu)

Yüksek

TURSign

Tanılma Yöntemleri

Yüksek

G
Ü
V
E
N
L

K

Zayıf

Zayıf

- Kripto Akıllı Kartlar
- Hardware Token
- Akıllı Kartlar
- ArcotID

- + Yüksek Seviyeli Tanılma
- + Kullanım Kolay ve Alınım
- + Taşınabilir (PDA, mobil, vs.)
- + Dijital İmza Atabilme
- + Çok Kolay ve Ucuz Kurulum
- + Kaybolmama ve Kırlmama

- Kullanıcı Adı
- + Şifre

KULLANIM

(son kullanıcı ve service provider)

Yüksek

TURSign

Ba ms z Kar la t rma

Buraya Yaz

Kullan c Ad
i ffe

Hardware
Token

Ak ll Kartlar

Arcot ID

0

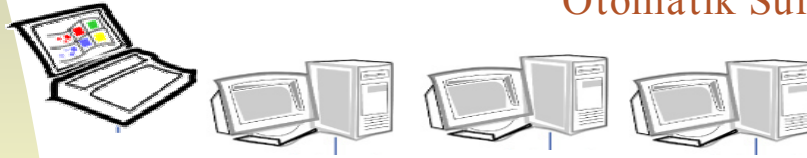


Bu işlem akışını malum bir çok dezavantajın yanında büyük maliyetlerde getirmektedir.

- Uygulamalara verilerin yeniden girilmesi = \$\$
- Dahil olan taraflara içeriğin dağıtılması = \$\$
- Kimlik onay = \$\$
- Verilerin Depolanması = \$\$

Başlangıç

Otomatik Süreçler



Otomatik

Manual

\$

\$

\$

\$

Tamamlandı

Başlangıç

Manual Süreç

TURSign

Otomasyon Bařlayıc 1

RDBMS

Veri Otomasyonu

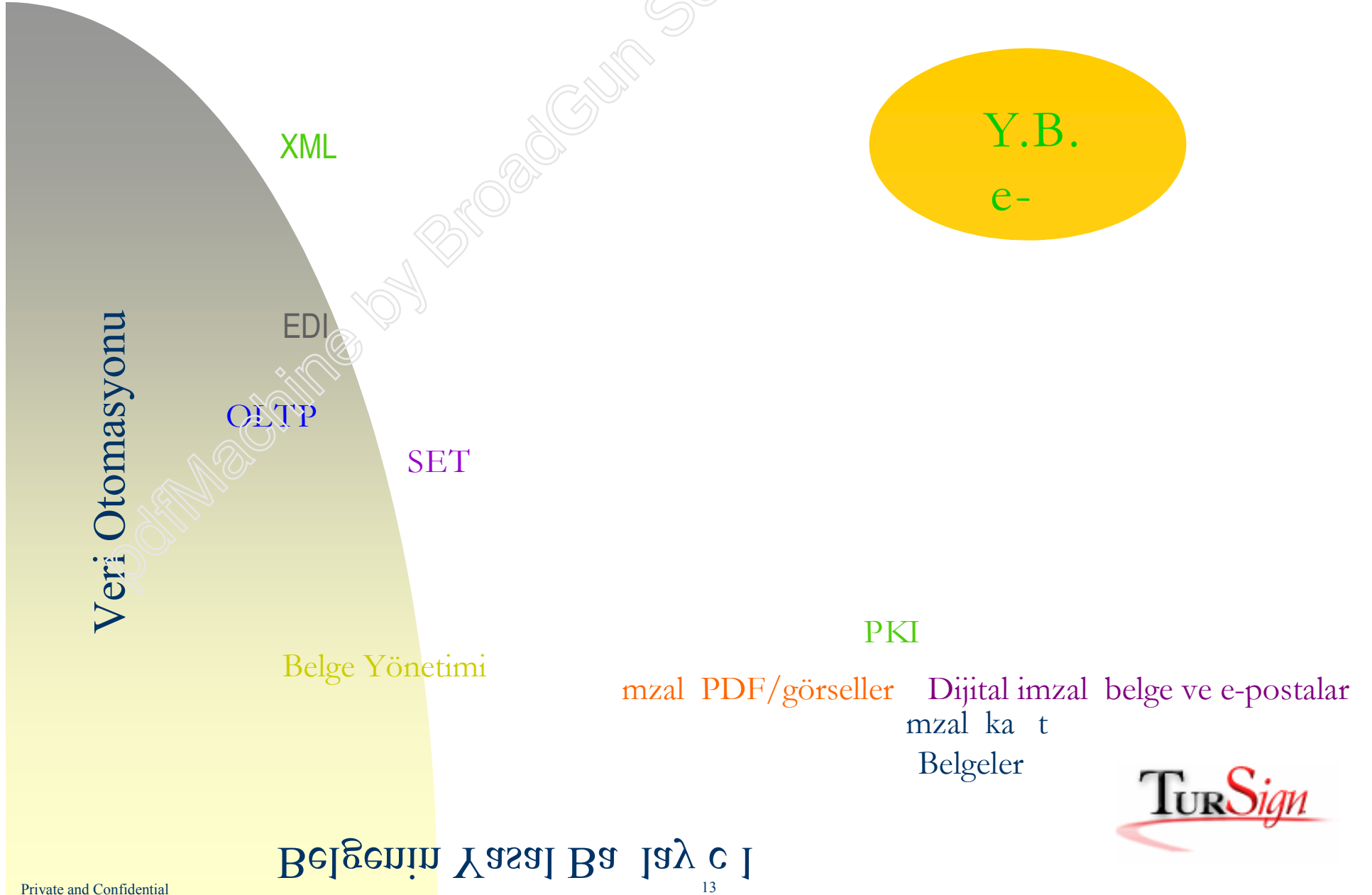
?

mzal Ka t
Belge

Belgenin Yasal Bařlayıc 1



Yasal Ba l ay c E- Pazar



Elektronik İmza Nedir?

Ses, Sembol, Süreç

- Tık, Pin, İfre
- Dijital Sertifika
- Akıllı Kart,
Biometrik



Ja User

Çerik Bütünlü ü ve nkar Edilememe Sa lama

Digital Signature özellikleri:

- Sadece imzay atan tarafından yaratılmalıdır
- Belgenin bütünlü ünü doğrulayacak bilgi içermelidir
- Yasal imza olduğu doğrulanabilmelidir

Nasıl Çalışır:

- Belge hakkında bilgi toplanır
- İmzalayan hakkında bilgi eklenir
- Bu bilgi imzalayanın özel anahtarı ile şifrelenir

İmza atarak...

- Herkes imzayı atan kişinin anonim anahtarı kullanarak imzayı doğrulayabilir
- Belge bütünlü ü imzada bulunan değer ile belgenin karşılaştırılması ile sağlanabilir.
- Belge şifrelenebilir ya da şifrelenmeyebilir.

Anonim Anahtar Edilememesi Nedir?



Cenk

Zeynep'in
Anonim Anahtar

Dear Ted:

Please invest £10,000
of my money in
Enron.

Carol



de ifre

ciphertext

```
011100111001001
110011100111001
001110000111111
```

Zeynep'in
Özel Anahtar



Zeynep

Dear Ted:

Please invest £10,000
of my money in
Enron.

Carol

ifre

pdfMachine by BroadGun Software

Te ekkür Ederim...

TUR*Sign*