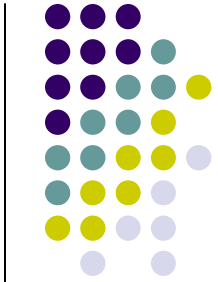


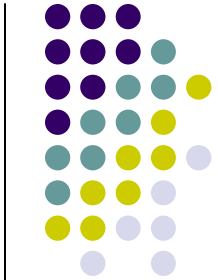
E- İMZA

Uğur Nasırlıel

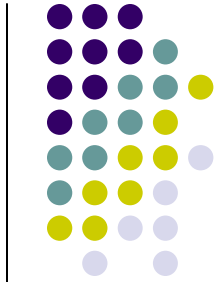
EMO Ankara Şubesi

Nisan 2008, Ankara

İÇERİK

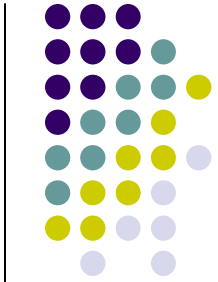


- İmza Nedir?
- E-Dönüşüm
- Hukuki Süreç
- E-imza



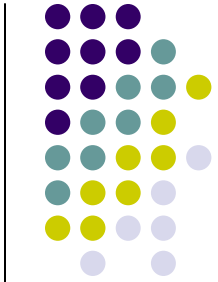
İMZA NEDİR?

İmza Nedir?



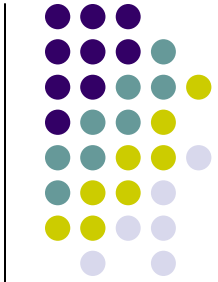
- İmza, bir kimsenin, bir yazının altına bu yazıyı yazdığını veya onayladığını belirtmek için her zaman aynı biçimde yazdığı ad veya işarettir.
- İmza, yazılı bir irade açıklamasının kendisine ait olduğunu ifade etmek amacıyla, bir kimsenin ismi için kullandığı özel biçimdeki çizgi ve harflerden kurulu bir işarettir.
- İmza, bir yazının altına kimin tarafından yazıldığını veya içeriğinin tasdik edildiğini belli etmek amacıyla konulan isim veya işarettir.
- 2525 sayılı Soyadı Kanunu'nun 2. maddesine göre imza ad ve soyad yazılmak suretiyle atılır.

İmzanın Önemi



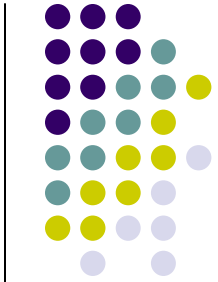
- İmza, öncelikle imzalayanın kimliğini belirlemektedir.
- Bir belge, bir şahsin el yazısı ile imzasını taşıyorsa, bu, belgenin onun tarafından oluşturulduğuna gösterir. Aksinin ispati imzalayana aittir.
- İmza, belge içeriğine ilişkin, imzalayanın niyetini ortaya koyar. Belgenin altında imzası bulunan kişinin belgenin içeriğini kabul ettiği varsayılır.
- Silinti ve kazıntı gibi bozulmalar olmadığı sürece, imza, imzalayanın bu şekilde bir belgenin oluşturulmasını istediği ve belgenin gerçeklik ve doğruluğunu (bütünlüğünü) gösterir.
- Her türlü resmi veya özel belgenin geçerlilik kazanabilmesi için üzerinde taşıması gereken en önemli unsurlardan biri imzadır.
- Yaşamımız boyunca binlerce kere attığımız imzamız, hukuk âleminde çok önemli sonuçlar doğuran bir işlemdir. Maddi değeri en yüksek varlığımız olan imzamız ile yüksek miktarda borç altına girebilir, tüm malvarlığınızı başka bir kimseye bağışlayabilir, pek çok suçu farkında olmadan işleyebilir ve daha birçok hukuki işlemi yapabiliriz.

Kimler İmza Atamaz?



- Bir âlet aracılığı ile atılan imza, ancak örf ve âdetçe kabul olunan hallerde ve özellikle çok miktarda tedavüle çıkarılan kıymetli evrakın imzalanması gereken durumlarda kabul edilir
- Körlerin imzaları, usulen tasdik olunmadıkça veya imza ettikleri zaman işlemin metnini bildikleri sabit olmadıkça geçerli değildir.
- Okuryazar ve imza atmasını bilen bir kişinin mühür kullanması geçerli değildir. Ayni şekilde parmak basması da kabul görmeyecektir.

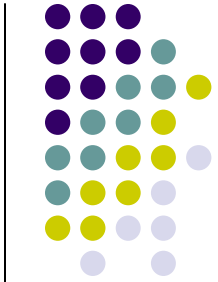
İmzanın Yeri



- İmzanın atılacağı yer hakkında Borçlar Kanununda her hangi bir hüküm bulunmamaktadır.
- İmza, bütün metnin benimsendiğini gösterecek şekilde metnin sonuna atılmalıdır.
- Böylece bize, metnin okunduğunu ve içeriğinin kabul edildiğini anlatır.
- Metnin üstüne, yanına, içine atılmış imzalar Kanunun aradığı sekil şartı açısından yetersizdir.
- Metinde sonradan yapılan ekleme ve çıkarmalar da ayrıca imzalanmalıdır. Aksi halde bu ilaveler geçerli olmayacaktır

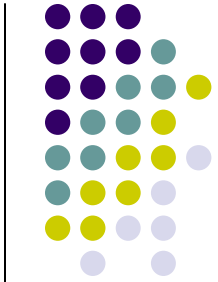
E- DÖNÜŞÜM

E-Dönüşüm Nedir?



- Bilgiye dayalı ekonominin hızla geliştiği ülkelerde kamu yönetimi ve yerel yönetimler; bilgiye dayalı yönetimler olma yönünde yapısal, yasal, yönetsel ve kültürel değişim ve dönüşüm yaşamaktadır.
- Bu dönüşümde bilgi ve iletişim teknolojileri önemli rol oynamaktadır.

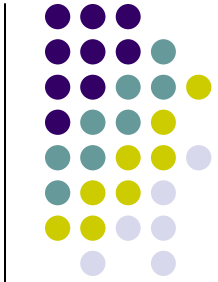
E-Dönüşüm Nedir?



- Mobil iletişim araçları, internet ve web teknolojileri, kamu yönetimine;
  - bilgi üretim ve yönetiminde,
  - etkileşimli çevrimiçi hizmetler üretme ve sunmada,
  - küresel düzeyde güvenlik yönetiminde
  - ekonomi yönetiminde ve
  - demokratik açılımlar sağlamada

  hem fırsatlar sunmakta hem de yeni tehditler getirmektedir.

E-Dönüşüm Nedir?



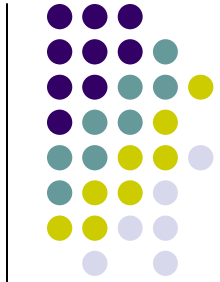
- Özellikle geniş coğrafyaya sahip ve nüfusu büyük olan ülkelerde bu işlevleri, manuel sistemlerle etkin ve verimli gerçekleştirmek zordur.
- Dünyada kamu yönetimleri de Bilişim Teknolojileri'nin olanaklarından yararlanarak, kamu yönetiminde etkinliği arttırma arayışına girmişlerdir.
- Bilişim Teknolojileri'nin, her alanda kullanımı toplumsal ve kurumsal e-dönüşümü zorunlu kılarak, yeni bir kavramın doğmasına neden olmuştur.
- Bu dönüşüm, Elektronik Devlet kavramını ortaya çıkarmıştır.

E-Dönüşümü Ortaya Çıkaran Gelişmeler

- Dünyanın gelişmiş ekonomilerinin bilgiye dayalı ekonomiye dönüşmesi ve ülkelerin bu yeni ekonomiden daha fazla pay alma arayışları,
- internetin tüm dünyada yaygınlık kazanması,
- vatandaşların bilgi ve hizmetlere ulaşmada kolay erişim, hız, ucuzluk ve şeffaflık talepleri,
- devletin etkin, şeffaf, hesap verir biçimde çalışmasını sağlayacak yönetsel reform çalışmalarının hız kazanması – Yeni Kamu İşletmeciliği
- az kaynakla çok iş yapma gereksinimi,
- devlete olan güveni artırma istemi.

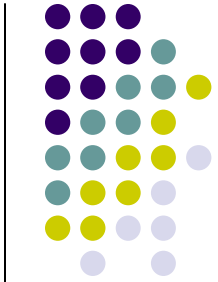
Toplumsal ve Kurumsal Düzeyde E-Dönüşüm

- **E-dönüşüm,**
  - gerek toplumsal düzeyde; gerek kamu yönetiminde kurumsal ve organizasyonel düzeyde gerçekleşmektedir.
- Toplumsal düzeyde dönüşüm ***"Bilgi Toplumu"*** kavramıyla; kurumsal ve organizasyonel dönüşüm ise ***"e-Devlet"*** kavramıyla açıklanmaktadır.



HUKUKİ SÜREÇ

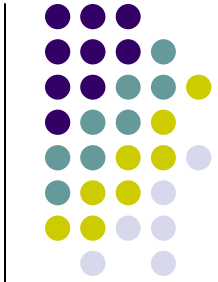
Hukuki Süreç



- E-İmza Kanunun hazırlığı, 1998'de Hazine ve Dış ticaret Müsteşarlığı tarafından başlatılmıştır.

- 2003 Haziran ayında TBMM gündemine giren e-imza kanun taslağı, 15 Ocak 2004'de TBMM Genel Kurul'unda yapılan görüşmede yasalaşmıştır.

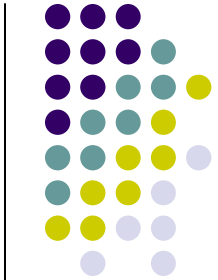
Hukuki Süreç



- 6 Ocak 2005 e-İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik 25692 Sayılı Resmi Gazete'de yayımı
- 27 Ocak 2005 Zorunlu Sertifika Mali Sorumluluk Sigortası Genel Şartları

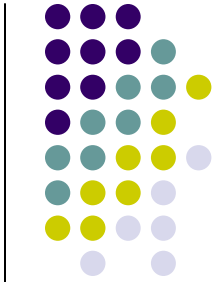
  Sertifika Mali Sorumluluk Sigortası Tarife ve Talimatı
- 19 Nisan 2006 2006/13 Sayılı Başbakanlık Genelgesi (Kamu Sertifikasyon Hizmetlerine İlişkin Usul ve Esaslar)

E-İmza Kanunu



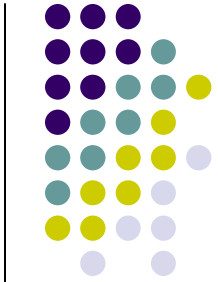
- Kanunun amacı, elektronik imzanın hukukî ve teknik yönleri ile kullanımına ilişkin esasları düzenlemektir.
- Kanun,
  - elektronik imzanın hukukî yapısını,
  - elektronik sertifika hizmet sağlayıcılarının faaliyetlerini ve
  - her alanda elektronik imzanın kullanımına ilişkin işlemleri kapsar.

E-İmza Kanunu



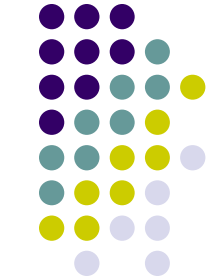
- Güvenli Elektronik İmza, Güvenli Elektronik İmza Oluşturma ve Doğrulama Araçları
- Elektronik Sertifika Hizmet Sağlayıcısı, Nitelikli Elektronik Sertifika ve Yabancı Elektronik Sertifikalar
- Denetim ve Ceza Hükümleri

Ülkemizde Bilişimle İlgili Olarak Gerçekleştirilen Hukuki Düzenlemeler



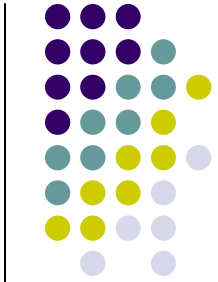
- **Doğrudan İlgili**
  - 5070 sayılı Elektronik İmza Kanunu,
  - 5369 sayılı Evrensel Hizmet Kanunu
- **Dolaylı İlgili**
  - 4982 sayılı Bilgi Edinme Hakkı Kanunu,
  - Yeni TCK
  - 4691 sayılı Teknoloji Geliştirme Bölgeleri Kanunu,
  - Tüketicinin Korunması Hakkında Kanun,
  - Nüfus Kanunu,
  - 5216 Sayılı Büyükşehir Belediyesi Kanunu

Hazırlıkları Devam Eden Kanun Tasarıları

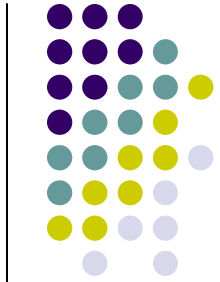


- Kişisel Verilerin Korunması Hakkında Kanun Tasarısı,
- Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarı

Neden E-imza'ya Geçiş

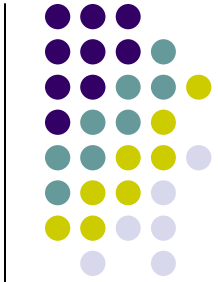


- Her alanda olduğu gibi, ticari hayat da artık elektronik ortama taşınmıştır. İnternet üzerinden yapılan sözleşmelerin ve pazarlamaların geçerliliği ve güvenliği için bir çok ülkede hukuki düzenlemelerin yapılması gereği doğmuştur. Bu yüzden Birleşmiş Milletler Uluslararası Ticaret Komisyonu tarafından hazırlanan, **"Örnek Elektronik Ticaret Kanunu"**, Birleşmiş Milletler genel kurulunda 16 Aralık 1996 tarihinde 51/162 sayılı karar ile kabul edilmiştir. Bu kanun, elektronik ticaret konusunda uluslararası ilk metindir ve elektronik ortamdaki diğer düzenlemelere de öncülük etmiştir. Kanunun 5. maddesinde belirtilen "**Bilgi, sırf sayısal veri olmasından dolayı hukuki sonuç, geçerlilik ve icra edilebilirlikten mahrum bırakılmamalıdır**" ifadesi ile sayısal verilerin hukuki boyutuna değinilmiş ve e-imza kavramının önü açılmıştır.



ELEKTRONİK İMZA

Elektronik İmza



- Elektronik imza, klasik imzaya tanınan işlevleri de kapsayan ve bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki veridir.
- **5070** Sayılı Elektronik İmza Kanunu'nda elektronik imza, "*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri*" şeklinde tarif edilmektedir (m.3/b).

Elektronik İmza

- Sayısal imzanın işlevi, elektronik ortamda sahte imzayı önlemek, belgelerin herhangi bir tahrifata uğramaksızın iletilmesini sağlamaktır.
- Sayısal imza, elektronik ortamın vazgeçilmez unsurlarından birisidir.
- Elle atılan imzanın taranarak dijital bir dokümana eklenmesi veya dijital kalemle imza atılması gibi durumlarda da elektronik imzadan bahsedilebilir.
- Bu anlamda elektronik imza, elektronik ortamda imzadan beklenilen fonksiyonları sağlamaktan uzaktır. Bu nedenle güvenli elektronik imzanın kullanılması önem arz etmektedir.

Güvenli Elektronik İmza Oluşturma Araçları

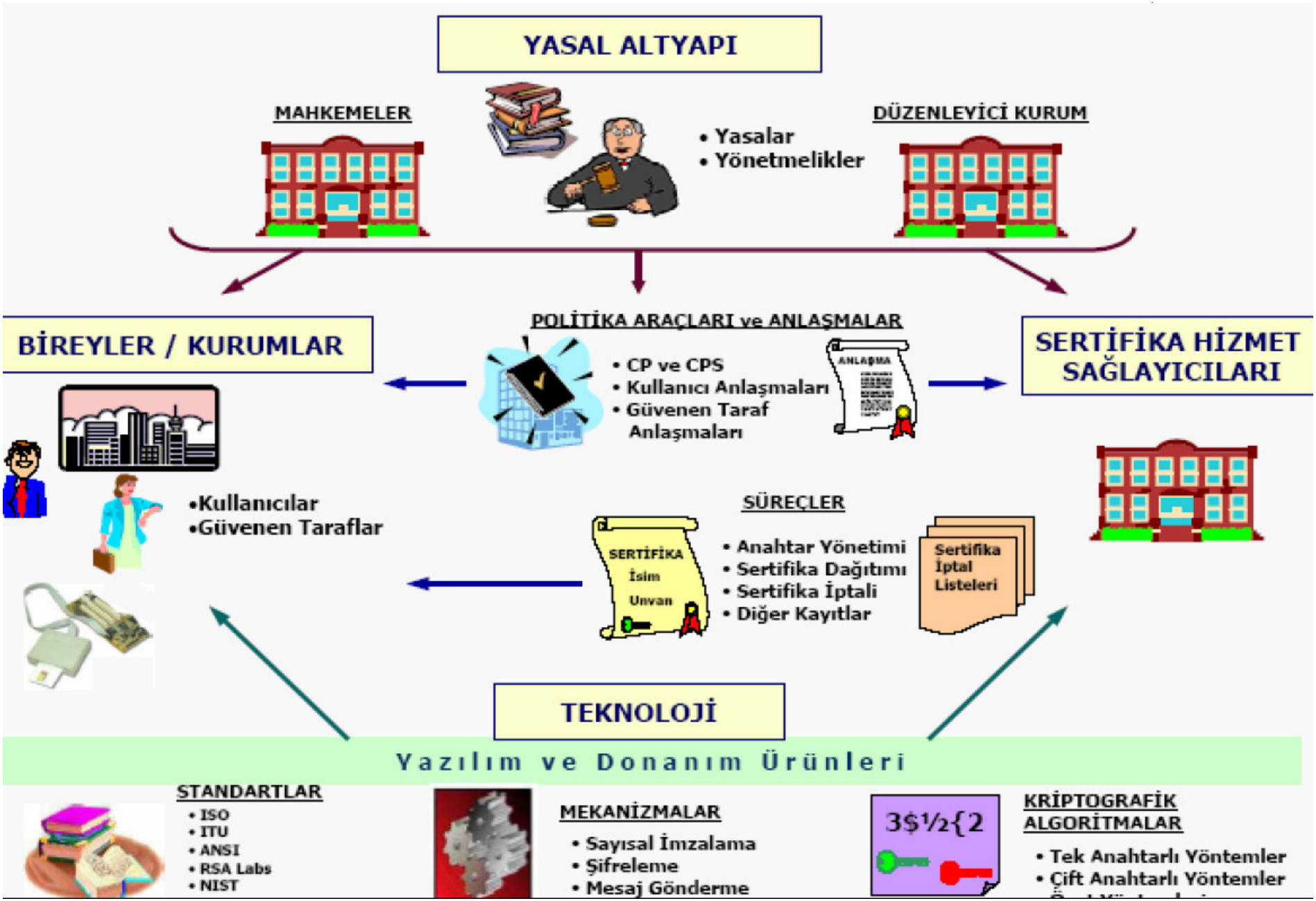
- Ürettiği elektronik imza oluşturma verilerinin kendi aralarında bir eşi daha bulunmamasını,
- Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin araç dışına hiçbir biçimde çıkarılamamasını ve gizliliğini,
- Üzerinde kayıtlı olan elektronik imza oluşturma verilerinin, üçüncü kişilerce elde edilememesini, kullanılamamasını ve elektronik imzanın sahteciliğe karşı korunmasını,
- İmzalanacak verinin imza sahibi dışında değiştirilememesini ve bu verinin imza sahibi tarafından imzanın oluşturulmasından önce görülebilmesini

sağlayan imza oluşturma araçlarıdır.

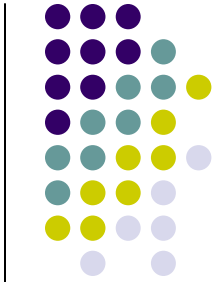
Elektronik İmza İle Yapılamayacak İşler

Güvenli elektronik imzanın hukukî sonucu ve uygulama alanı

- MADDE 5. — Güvenli elektronik imza, elle atılan imza ile **aynı hukukî** sonucu doğurur.
- Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmeleri güvenli elektronik imza ile gerçekleştirilemez.

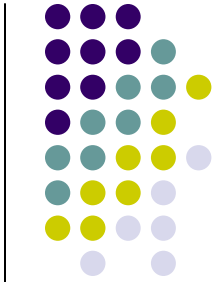

YASAL ALTYAPI
MAHKEMELER
• Yasalar
• Yönetmelikler
DÜZENLEYİCİ KURUM
BİREYLER / KURUMLAR
POLİTİKA ARAÇLARI ve ANLAŞMALAR
• CP ve CPS
• Kullanıcı Anlaşmaları
• Güvenen Taraf Anlaşmaları
ANLAŞMA
SERTİFİKA HİZMET SAĞLAYICILARI
•Kullanıcılar
•Güvenen Taraflar
SÜREÇLER
SERTİFİKA
İsim
Unvan
• Anahtar Yönetimi
• Sertifika Dağıtımı
• Sertifika İptali
• Diğer Kayıtlar
Sertifika İptal Listeleri
TEKNOLOJİ
Yazılım ve Donanım Ürünleri
STANDARTLAR
• ISO
• ITU
• ANSI
• RSA Labs
• NIST
MEKANİZMALAR
• Sayısal İmzalama
• Şifreleme
• Mesaj Gönderme
KRİPTOGRAFİK ALGORİTMALAR
• Tek Anahtarlı Yöntemler
• Çift Anahtarlı Yöntemler

Sertifikasyon Süreci



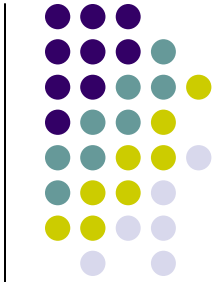
- **Elektronik Sertifika Sağlayıcısının Yükümlülükleri**
  - Nitelikli sertifika verdiği kişilerin kimliğini resmî belgelere göre güvenilir bir biçimde tespit etmekle (md. 10),
  - Kişilerin kimliği; nüfus cüzdanı, pasaport, sürücü belgesi gibi fotoğraflı ve geçerli resmi belgelere göre tespit edilir. Kişi, kimlik tespiti esnasında bizzat hazır bulunur (Yön. md.9).
  - Kurumsal başvuru - Kurumsal başvuru sahibi, adına başvuruda bulunduğu kişilerin nitelikli elektronik sertifika taleplerini yazılı olarak belgelendirir (Yön.md. 9).

Sertifikasyon Süreci



- Sertifika sahibinin diğer bir kişi adına hareket edebilme yetkisi, meslekî veya diğer kişisel bilgilerinin sertifikada bulunması durumunda, bu bilgileri de resmî belgelere dayandırarak güvenilir bir biçimde belirlemekle (K. Md.10)
- Elektronik sertifika hizmet sağlayıcısı üretilen imza oluşturma verisinin bir kopyasını alamaz veya bu veriyi saklayamaz (K. md.10)
- Nitelikli elektronik sertifika, geçerlilik süresinin sona ermesinden önce sertifika sahibinin veya sertifika sahibinin onayını almak koşuluyla kurumsal başvuru sahibinin talebi doğrultusunda ESHS tarafından yenilenebilir (Yön. md.12)

Sertifikasyon Süreci

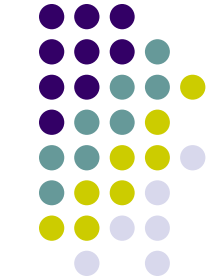


- **Nitelikli Elektronik Sertifika Sahibinin Yükümlülükleri**
  - Sertifika oluşturmak için gerekli belgeleri ESHS'ye eksiksiz olarak vermek ve bunları güncellemek
  - İmza oluşturma ve doğrulama verilerini sadece elektronik imza oluşturma ve doğrulama amaçlı olarak ve sertifikanın kullanım ve maddi sınırlamaları dahilinde kullanmak
  - İmza oluşturma verisinin ve imza oluşturma aracına erişim verisinin gizliliğini sağlamak ve bunlar ile imza oluşturma aracının kaybolması, çalınması, güvenilirliğinden şüphe edilmesi durumunda ESHS'yi derhal bilgilendirmekle

Ülkemizde Elektronik Sertifika Hizmet Sağlayıcıları

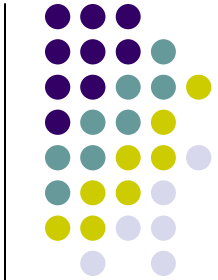
- Elektronik Bilgi Güvenliği A.Ş. -E-Güven, 2005
- TUBİTAK-UEKAE -Kamu Sertifikasyon Merkezi, 2005
- TürkTrust Bilgi, İletişim ve Bilişim Güvenliği Hizmetleri A.Ş, 2005
- EBG Bilişim Teknolojileri ve Hizmetleri A.Ş. (e-Tugra), 2006

Üçüncü Kişilerin Yükümlülükleri



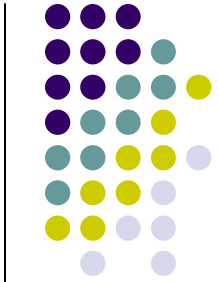
- Sertifikanın “nitelikli elektronik sertifika” olup olmadığını kontrol etmek
- Sertifikanın iptal ve geçerlilik durumunu kontrol etmek
- Sertifikanın kullanımına yönelik bir kısıtlamanın olup olmadığını kontrol etmek
- Güvenli e-imza doğrulama aracını kullanmak

Kurumun Yükümlülükleri



- Bildirimin incelenmesi
- Denetimin yapılması
- İlgili ücretlerin belirlenmesi
- ESHS'nin faaliyetinin sonlandırılması
- Düzenlemelerin gözden geçirilmesi ve güncellenmesi
- Elektronik imzaya ilişkin yaptığı çalışmalarla ve sektörün durumuyla ilgili yıllık durum rapor hazırlaması
- ESHS'lerin bildirim sürecine ve faaliyet durumuna ilişkin bilgileri internet sayfasında yayımlaması

Bilgilerin Korunması

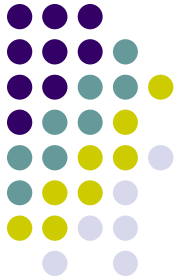


- Elektronik sertifika talep eden kişiden, elektronik sertifika vermek için gerekli bilgiler hariç bilgi talep edemez ve bu bilgileri kişinin rızası dışında elde edemez.
- Elektronik sertifika sahibinin izni olmaksızın sertifikayı üçüncü kişilerin ulaşabileceği ortamlarda bulunduramaz,
- Elektronik sertifika talep eden kişinin yazılı rızası olmaksızın üçüncü kişilerin kişisel verileri elde etmesini engeller. Bu bilgileri sertifika sahibinin onayı olmaksızın üçüncü kişilere iletemez ve başka amaçlarla kullanamaz (K. 12).

İmza Oluşturma Verilerinin İzinsiz Kullanımı

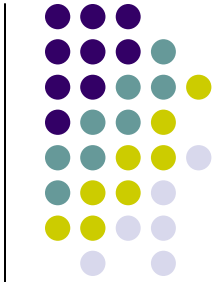
- Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında;
  - Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile yetkisi olmadan elektronik sertifika oluşturanlar veya bu elektronik sertifikaları bilerek kullananlar,fiilleri başka bir suç oluştursa bile ayrıca, iki yıldan beş yıla kadar hapis ve birmilyar liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.
  - Yukarıdaki fıkrada işlenen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.
  - Bu maddedeki suçlar nedeniyle oluşan zarar ayrıca tazmin ettirilir.

Elektronik Sertifikalarda Sahtekârlık



- Tamamen veya kısmen sahte elektronik sertifika oluşturanlar,
- geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler,
- yetkisi olmadan elektronik sertifika oluşturanlar,
- bu elektronik sertifikaları bilerek kullananlar,
- fiilleri başka bir suç oluştursa bile ayrıca, iki yıldan beş yıla kadar hapis ve bir milyar liradan aşağı olmamak üzere ağır para cezasıyla cezalandırılırlar.
- Yarı oranında arttırım ve tazmin

Elektronik İmza Çeşitleri



1- Basit Elektronik İmza:

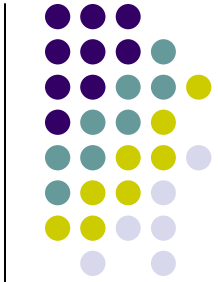
- Basit elektronik imza bize sadece verinin bütünlüğünün korunduğunu göstermektedir. Basit elektronik imzaya örnek olarak bilgisayar ekranına kalemle atılan imza veya el yazısıyla imzanın tarayıcıdan geçirilerek elektronik belgelere eklenmesi gösterilebilir.

Elektronik İmza Çeşitleri

2. Gelişmiş Elektronik İmza:

- Gelişmiş elektronik imza, genel olarak elektronik imza tanımından yola çıkılarak, bu tanıma çeşitli unsurların eklenmesi suretiyle yapılmaktadır. Gelişmiş elektronik imza verinin bütünlüğünü korumasının yanında imzalayanının kimlik tespitine de imkân sağlar.
- 5070 sayılı Elektronik İmza Kanunu'nda gelişmiş elektronik imzaya yer verilmemiştir. Ancak Direktifte sayılan unsurlar Kanunun 4'üncü maddesinde sayılan güvenli elektronik imzanın unsurları arasında yer almaktadır.

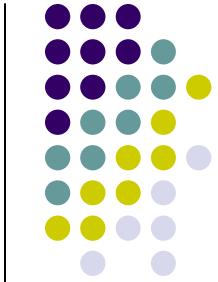
Elektronik İmza Çeşitleri



3. Güvenli Elektronik İmza:

- Güvenli elektronik imza, gelişmiş elektronik imzanın unsurlarını içermekle birlikte nitelikli elektronik sertifikaya dayanmakta ve güvenli imza oluşturma araçları ile oluşturulmuş imzadır. Direktifin 5'inci maddesine göre bu unsurların varlığı halinde, üye ülkeler bu imzanın el yazısı ile imzaya eşdeğerliğini ve yargılamada delil olarak kullanılmasını sağlayacaklardır.
- Elektronik İmza Kanununda "*nitelikli elektronik imza*" kavramı yerine "*güvenli elektronik imza*" kavramı tercih edilmiş, gelişmiş elektronik imza güvenli elektronik imza ayrımına gidilmemiştir. Güvenli elektronik imzanın unsurları 4'üncü maddede sayılmıştır.

Elektronik İmza Çeşitleri



Güvenli elektronik imza:

MADDE 4. — Güvenli elektronik imza;

a) Sadece imza sahibine bağlı olan,

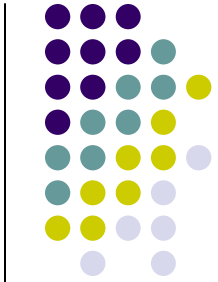
b) Sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan,

c) Nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan,

d) İmzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan,

Elektronik imzadır.

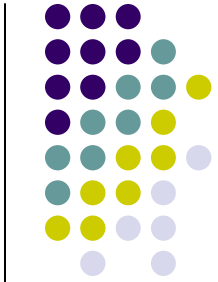
Elektronik İmza Çeşitleri



4. Akredite Edilmiş Sertifika Hizmet Sağlayıcısı Tarafından Verilen İmza

- Elektronik sertifika hizmet sağlayıcıları açısından Avrupa Birliği Direktifinde akreditasyon sistemi öngörülmüş olmasına rağmen hukukumuzda buna yer verilmemiştir. İhtiyari akreditasyon, bir sertifika hizmet sağlayıcısı için özel hak ve yükümlülüklere bağlı olarak izin verilme usulüdür.
- Türk hukuk sisteminde elektronik sertifika sağlayıcı olmada başvurudan sonra 2 ay bekleme, akreditasyon sisteminin getirilmemesi eleştirilere konu olmuştur.

Şifreleme



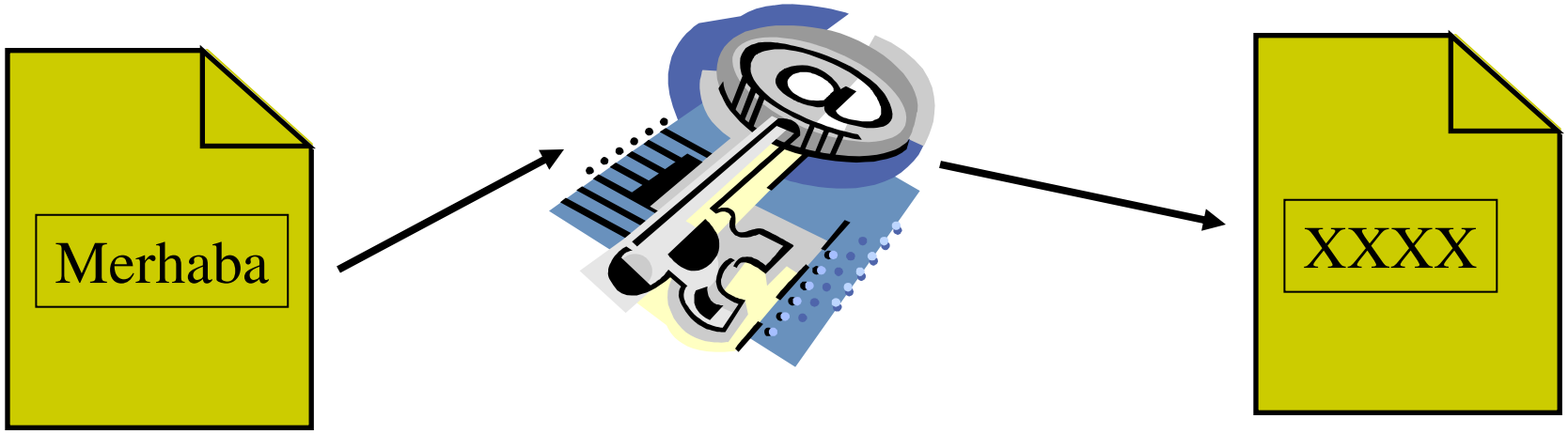
Sezar şifresi

- Harf=harf+2
- MESUT OGTVÜ

Simgeleme

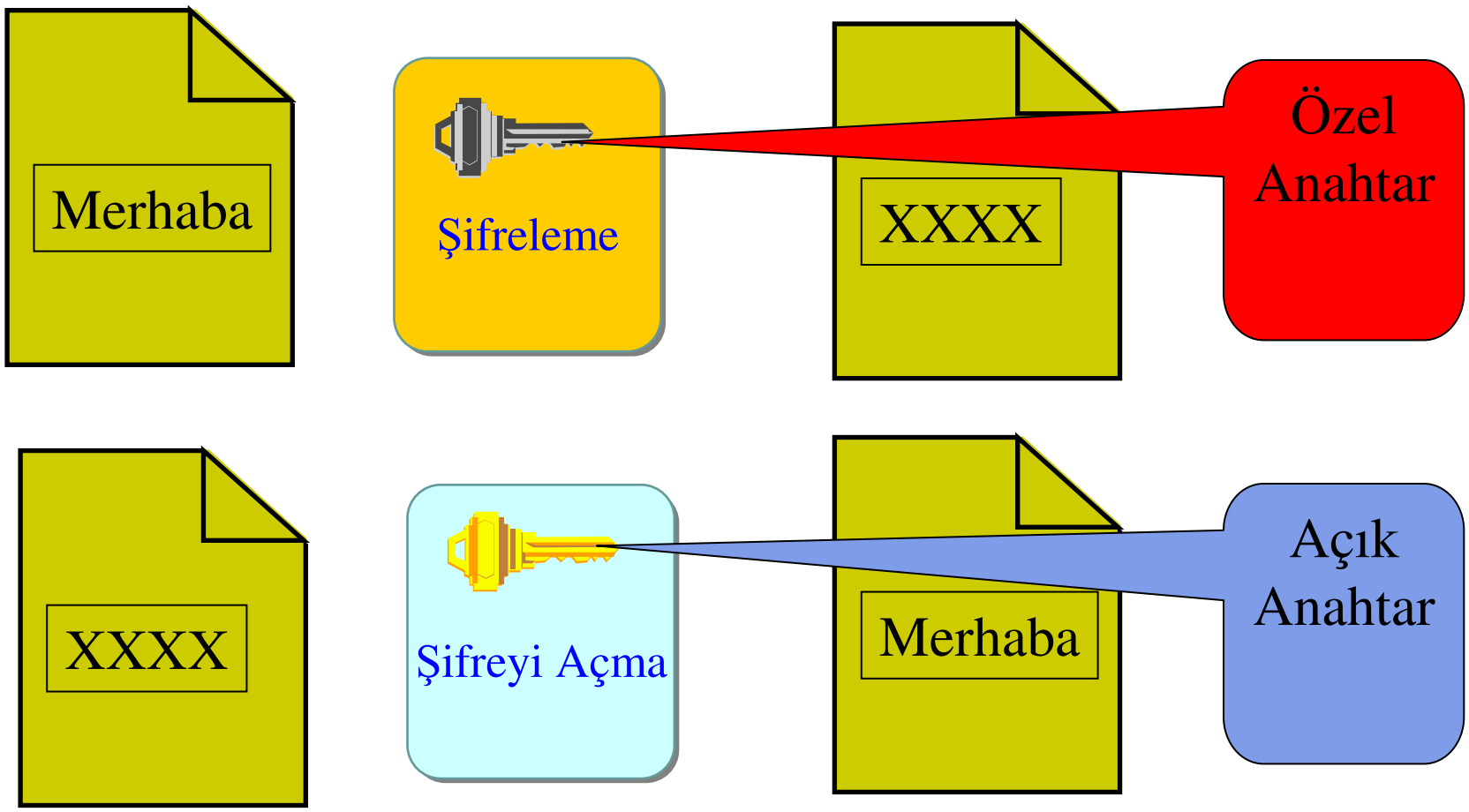
- A B, B C, ... Y Z, Z A
- MESUT NFŞÜU

Tek Anahtarlı Algoritmalar İle Şifreleme

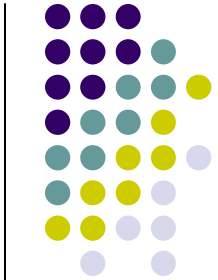


Dökümanı şifrelemek ve açmak için **aynı** anahtar kullanılır.

Çift Anahtarlı Algoritmalar İle Şifreleme

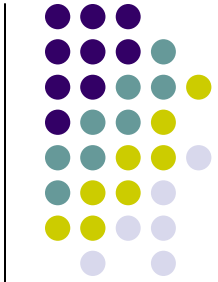


Açık Anahtar Şifreleme



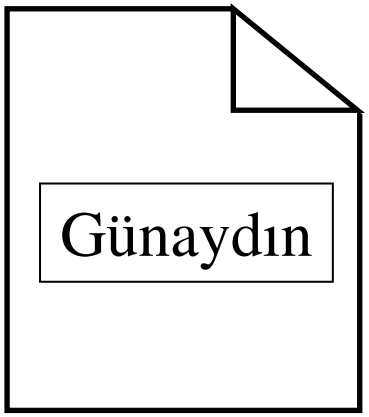
- Açık anahtar şifrelemede, özel ve açık olmak üzere bir anahtar çifti vardır. Kişi kendi özel anahtarını gizli tutarken, açık anahtarını şifreli iletişim kuracağı kişilere iletir.
- Bu anahtarlar birbirine matematiksel bir ilişkiyle bağlanmıştır fakat; anahtarlardan birini kullanarak diğerini elde etmek çok zor hatta imkansızdır.
- Anahtarlardan açık olanıyla şifrelenen bir veri ancak bu açık anahtara karşılık gelen özel anahtarla açılabilir.

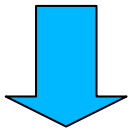
Açık Anahtar Altyapısı



- Asimetrik şifreleme yöntemidir: şifreleyen ve şifreyi çözen anahtar (sayı) farklıdır. Bu yönden simetrik şifrelemeye göre daha güvenlidir.
- Anahtarlar çiftler halinde üretilir. Açık anahtarın şifrelediği sadece gizli anahtar tarafından, gizli anahtarın şifrelediği ise sadece açık anahtar tarafından çözülebilir.

Hash (Özet) Algoritması



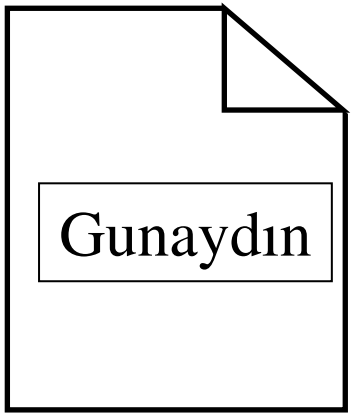


1A^#G

Özet algoritmaları

- Mesajı her zaman ve aynı uzunlukta bir özete indirger
- Özetten yola çıkarak mesaj yeniden elde edilemez
- İki farklı mesajın özeti aynı olmaz

(SHA-1, MD4, MD5)

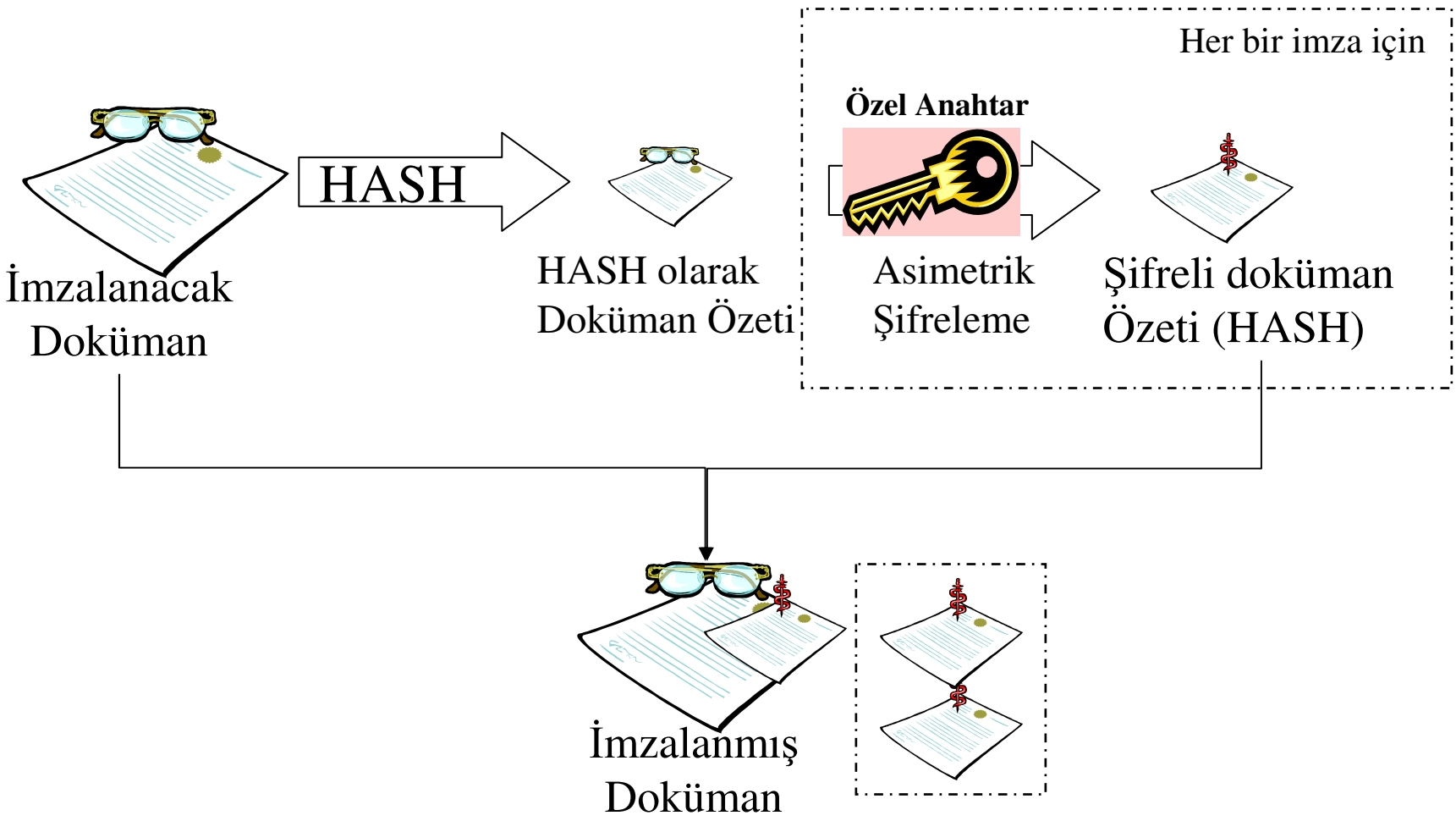


&RT1Y

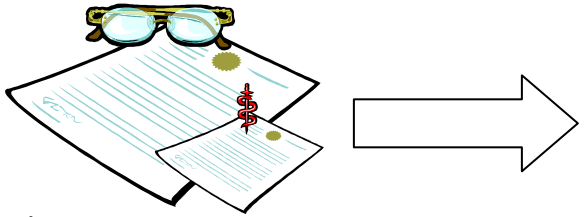
Elektronik İmza

- Hangi anahtar çiftinin kime ait olduğunun bilinmesi
  - Anahtar çifti üretimi
  - Doğru kimlik tespiti
- Güvenilir bir kurum tarafından anahtar çiftinin (doğrulama verisinin) kime ait olduğunun beyanı
  - Elektronik sertifika

Elektronik İmza Prosedürü

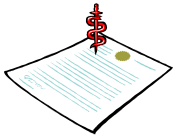


Elektronik İmza Doğrulama



İmzalanmış Doküman

Kontrol edilecek Doküman



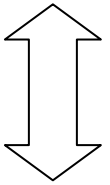
Şifreli doküman Özeti (HASH)

HASH

Genel Anahtar

Şifre çöz

HASH olarak Doküman Özeti

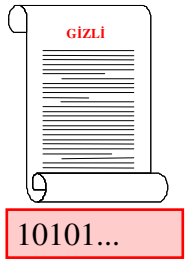


=?

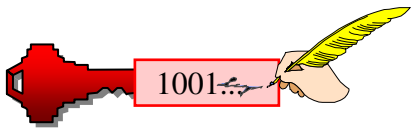
Gelen Doküman Özeti

İmzalama-Doğrulama Süreci

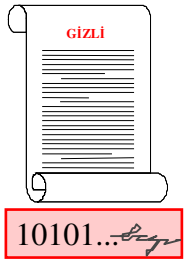
İmzalama Süreci



1. Orijinal verinin mesaj Özetini (hash değerini) hesapla

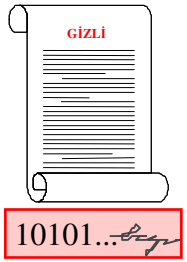


2. Mesaj özetini kendi özel anahtarınla şifrele (imzala)



3. İmzalanmış orijinal veri meydana gelir.

Doğrulama Süreci



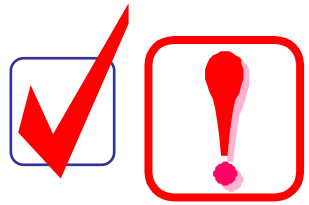
1. Mesaj özetini yeniden hesapla

1001...

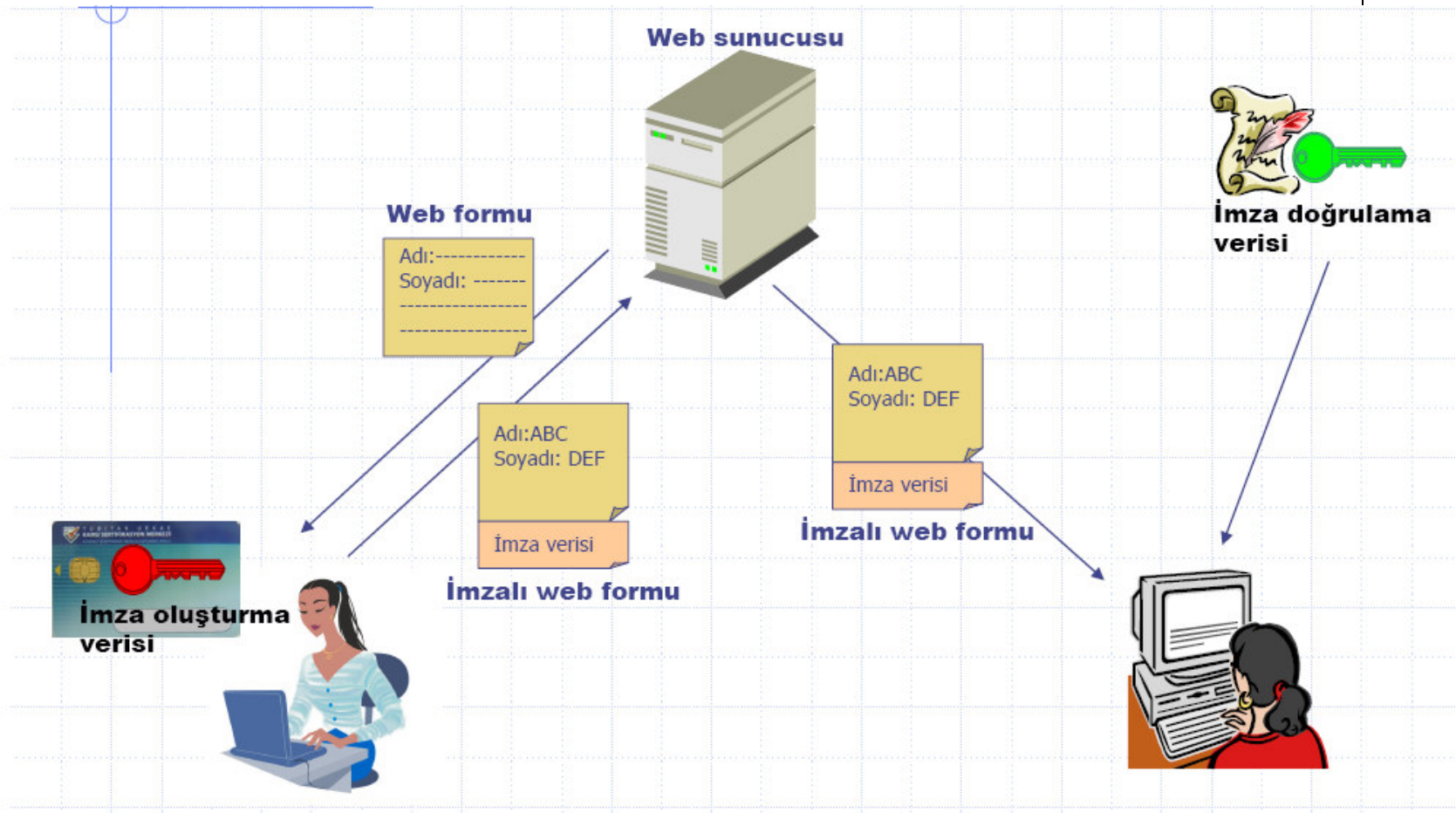
2. Karşı tarafın açık anahtarını kullanarak, şifrelenmiş orijinal mesaj özetini aç

1001... =? 1001...

3. Kendi hesapladığın mesaj özetiyle, orijinal mesaj özetini karşılaştır



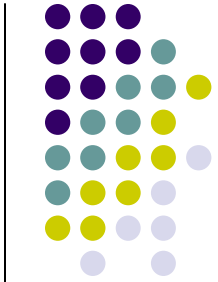
Örnek Web Uygulaması



Sonuç

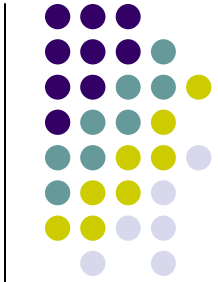

Gizlilik
Bütünlük ve İnkar Edememe
Kimlik Doğrulama
Şifreleme
Sayısal İmza
Sayısal İmza
Açık Özel Anahtarlar
Sertifikalar
Standartlara Uygun
Kayıt Tutulabilir
Yönetilebilir
Açık Anahtar Altyapısı

Sonuç

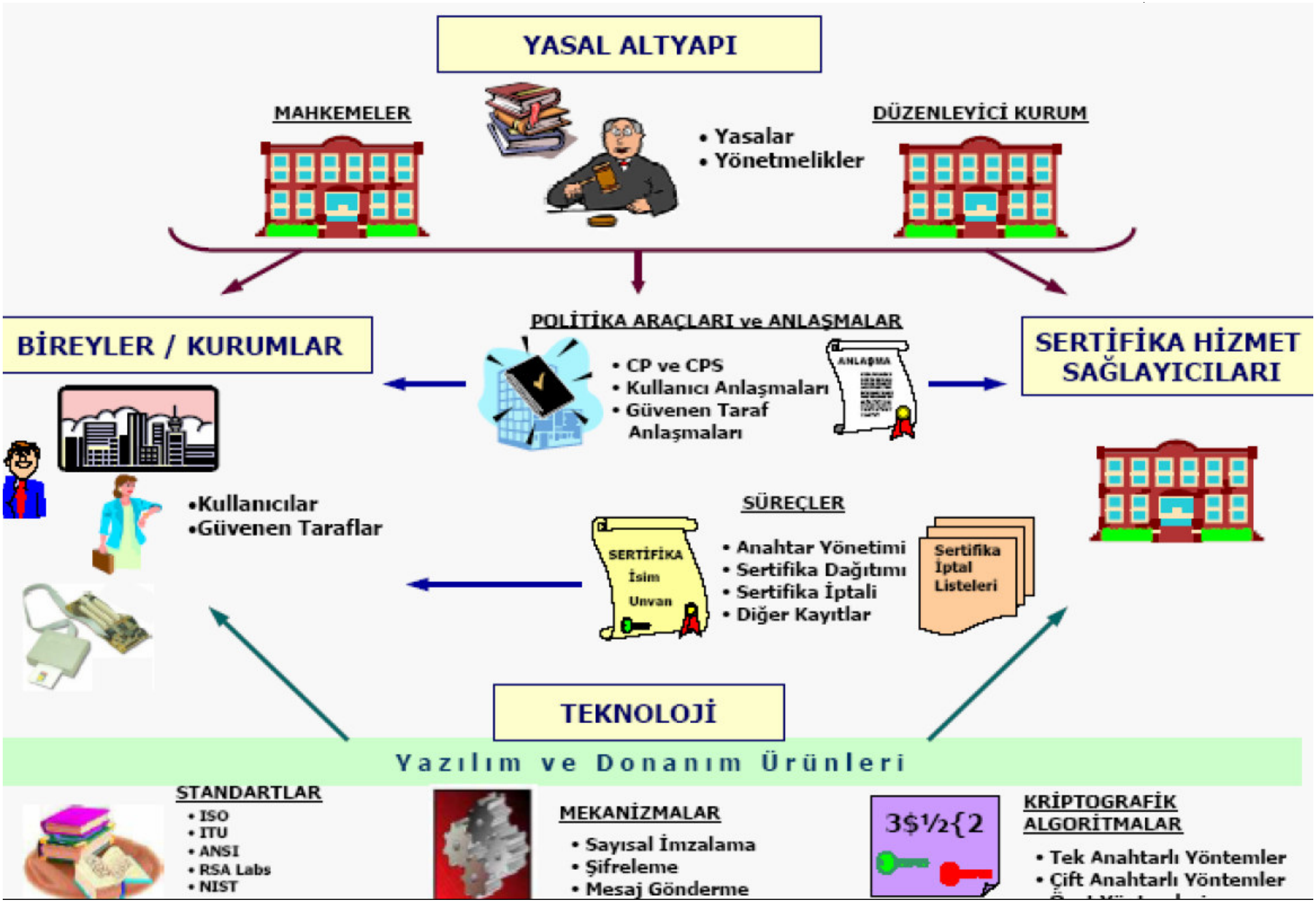


- **Gizlilik:** Bilginin istenmeyen kişiler tarafından anlaşılması engellenir.
- **Bütünlük:** Bir iletinin alıcısı bu iletinin iletim sırasında değişikliğe uğrayıp uğramadığını öğrenmek isteyebilir;
- **Reddedilemezlik:** Bilgiyi oluşturan ya da gönderen, daha sonra bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkâr edememelidir.

Sonuç



- **Kimlik Belirleme ve Kimlik Denetimi:** Kimlik belirleme ve kimlik denetimi, kriptografinin en yaygın kullanım alanlarından birisidir. Kimlik belirleme, birinin ya da bir şeyin kimliğinin doğrulanmasıdır.
- **Güvenli iletişim:** Güvenli iletişim, iki tarafın birbirine gönderdiği mesajları şifrelemesi yoluyla, mesajları, istenmeyen üçüncü kişilerin okumasını engellemesidir.


YASAL ALTYAPI
MAHKEMELER
• Yasalar
• Yönetmelikler
DÜZENLEYİCİ KURUM
BİREYLER / KURUMLAR
POLİTİKA ARAÇLARI ve ANLAŞMALAR
• CP ve CPS
• Kullanıcı Anlaşmaları
• Güvenen Taraf Anlaşmaları
ANLAŞMA
SERTİFİKA HİZMET SAĞLAYICILARI
•Kullanıcılar
•Güvenen Taraflar
SÜREÇLER
SERTİFİKA
İsim
Unvan
• Anahtar Yönetimi
• Sertifika Dağıtımı
• Sertifika İptali
• Diğer Kayıtlar
Sertifika İptal Listeleri
TEKNOLOJİ
Yazılım ve Donanım Ürünleri
STANDARTLAR
• ISO
• ITU
• ANSI
• RSA Labs
• NIST
MEKANİZMALAR
• Sayısal İmzalama
• Şifreleme
• Mesaj Gönderme
KRİPTOGRAFİK ALGORİTMALAR
• Tek Anahtarlı Yöntemler
• Çift Anahtarlı Yöntemler

Kaynakça

- Doç. Dr. Türksel KAYA BENSGHİR, TODAİE, Aralık 2006, Ankara
- Mesut ORTA (Hakim), TODAİE, Aralık 2006, Ankara
- İnci BİÇKİN (Yargıtay Teknik Hakimi) Bilişim ve Hukuk Dergisi
- Stj. Av Emrah YAVUZCAN, Bilişim ve Hukuk Dergisi

TEŞEKKÜRLER