



TODAİE eDEVLET MERKEZİ UYGULAMALI E-İMZA SEMİNERİ 16-17 KASIM 2011

E-imza Teknolojisi

TODAİE Sunumu

Ferda Topcan
Başuzman Araştırmacı
ferdat@uekae.tubitak.gov.tr
(312) 4688486-19

İçerik

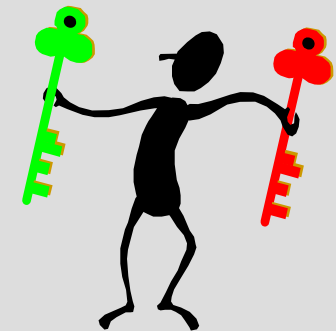
- Açık Anahtarlı Altyapı Teknolojisi
 - Çift (Açık) Anahtarlı Algoritmalar
 - Özet Algoritmaları
- Elektronik İmza
- Elektronik Sertifika ve Elektronik Sertifika Hizmet Sağlayıcıları



Açık Anahtarlı Altyapı Teknolojisi

Açık Anahtarlı Altyapılar (*Public Key Infrastructure -PKI*)

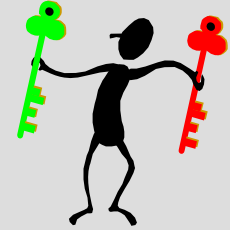
- Matematiksel şifreleme yöntemleri kullanılır.
- Şifreleme algoritması gizli değildir.
 - Algoritmanın güvenliği, çözülmesi mümkün olmayan matematiksel problemlere dayanır.
- Şifreleme ve şifre çözme için büyük sayı dizilerinden oluşan 2 anahtar kullanılır.
- Güvenlik, anahtardan birisinin gizliliğine bağlıdır.



Çift (Açık) Anahtarlı Algoritmalar

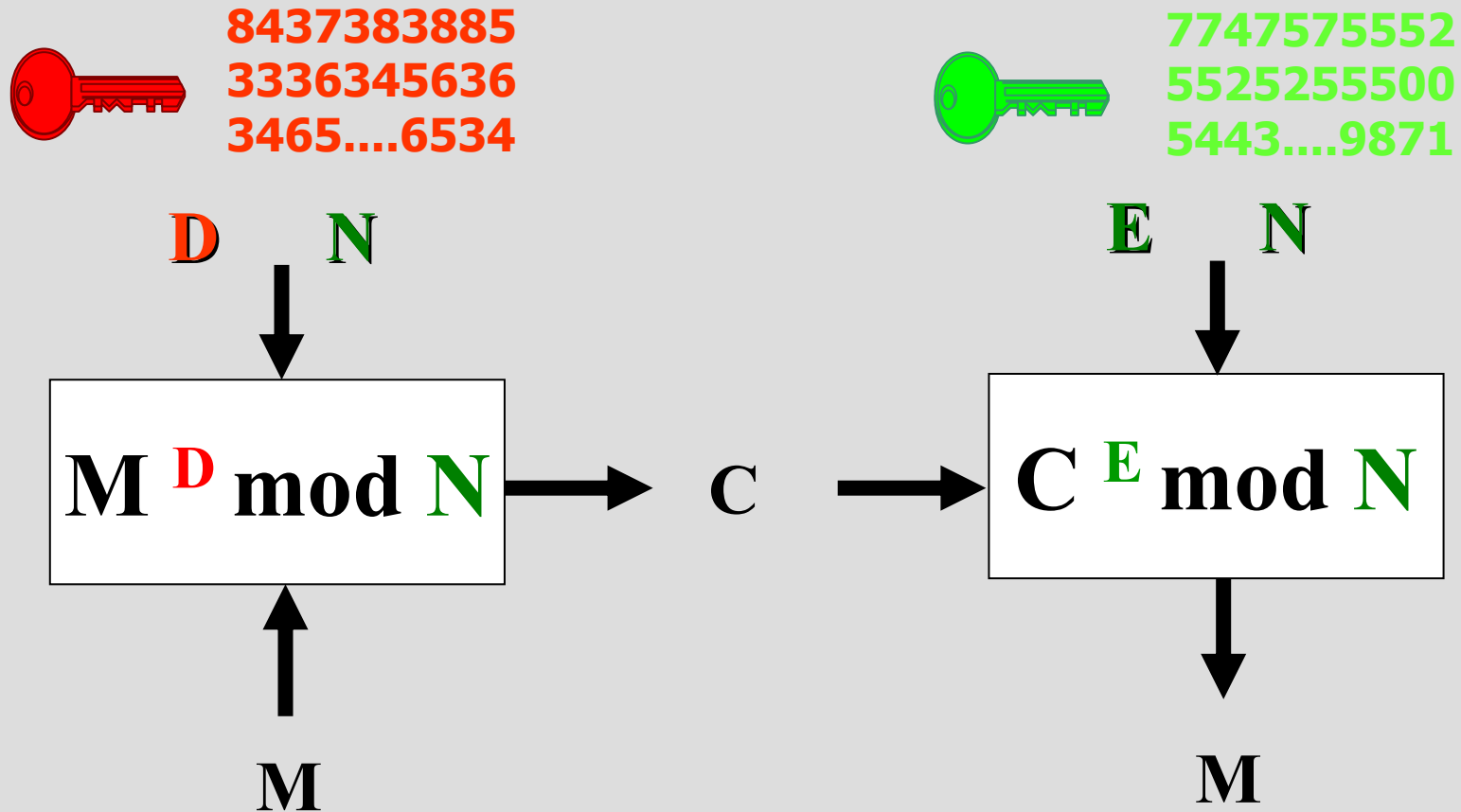
Çift anahtarlı kriptografik algoritmaların kullanımında her kullanıcıya 2 anahtar verilir:

- **Özel Anahtar**: Gizli tutulması gereken bir bilgidir.
- **Açık Anahtar**: Gizli tutulması gerekmeyen açık bir bilgidir.
- Anahtarlar kullanılacak algoritmaya bağlı olarak birlikte oluşturulur.
- İki anahtar arasında matematiksel bir ilişki vardır. Birisi ile şifrelenen veri sadece ve sadece diğeri ile çözülebilir.
- Açık anahtara bakarak özel anahtarın elde edilmesi mümkün değildir.
- Üretilen her anahtar çifti eşsizdir.

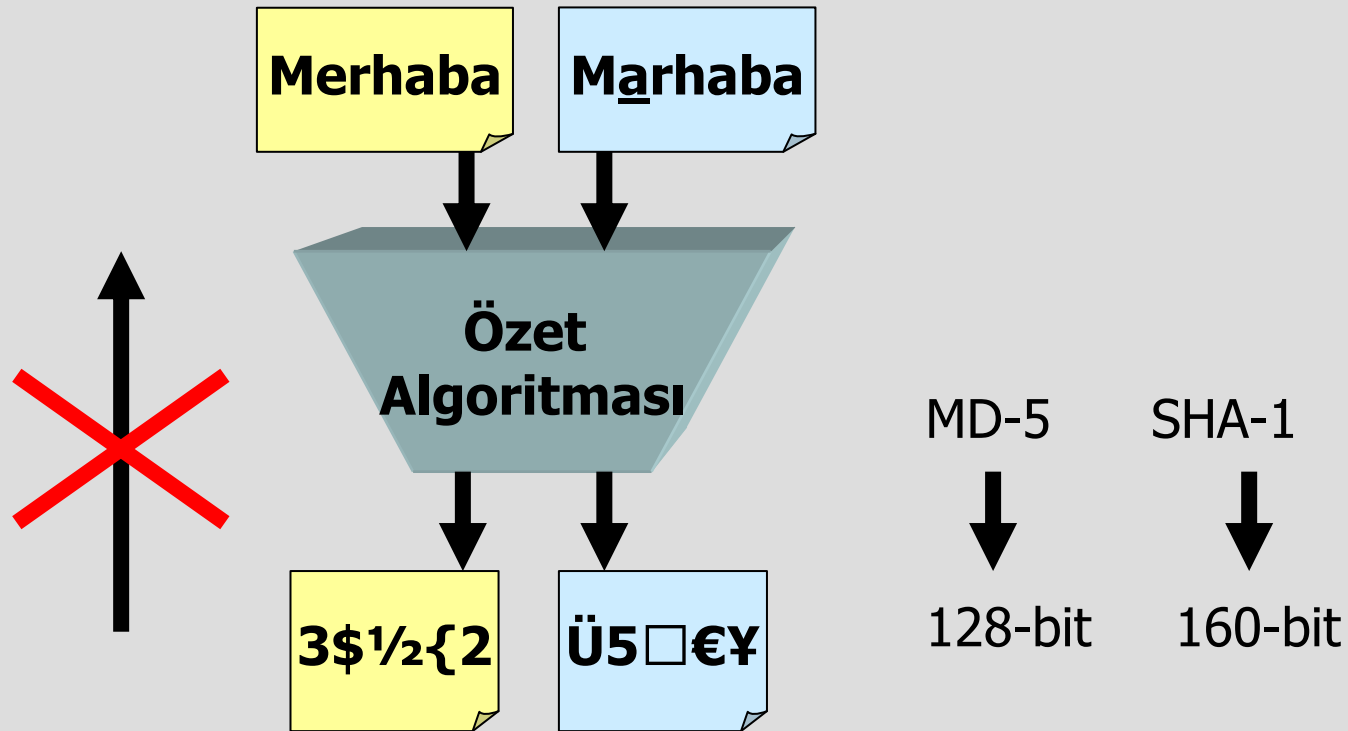


- **RSA (Rivest Shamir Adleman)**
- **DH (Diffie Hellman)**
- **DSA (Digital Signature Algorithm)**
- **Eliptik Eğri Algoritmaları**

Algoritma Yapısı (RSA)



Özet Algoritmaları



1. Farklı mesajlar için farklı özetler elde edilir
2. Özet değeri mesajdan bağımsız olarak sabit uzunluktadır
3. Özetten mesaj geri elde edilemez



Elektronik İmza

Elektronik İmza



5070 sayılı Kanun'daki tanım:

“Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri”

Yasal olmayan elektronik imzalar:

- Kağıt üzerindeki imzanın elektronik ortama aktarılmasıyla oluşturulan resim
- Parmak izinin elektronik ortama aktarılması
- Ekran atılan imza
- VS.. VS..

Kullanılan Teknoloji

Açık Anahtarlı Altyapı Teknolojisi

1. Çift anahtarlı kriptografik bir algoritma kullanılır. (RSA, DSA, vs..)
2. Özet algoritması kullanılır. (SHA, RIPEM, vs..)

Mevzuata göre kullanılabilecek çift anahtarlı kriptografik algoritmalar ve anahtar uzunlukları:

- RSA için en az 1024 bit veya
- DSA için en az 1024 bit veya
- DSA Eliptik Eğrisi için en az 163 bit

Mevzuata göre kullanılabilecek özet algoritmaları:

- RIPEMD – 160 veya
- SHA – 1 veya
- SHA-224 veya
- SHA-256 veya
- WHIRLPOOL

İmza Sahibine ait Anahtarlar

Özel anahtar (imza oluşturma verisi)

“İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi veriler”

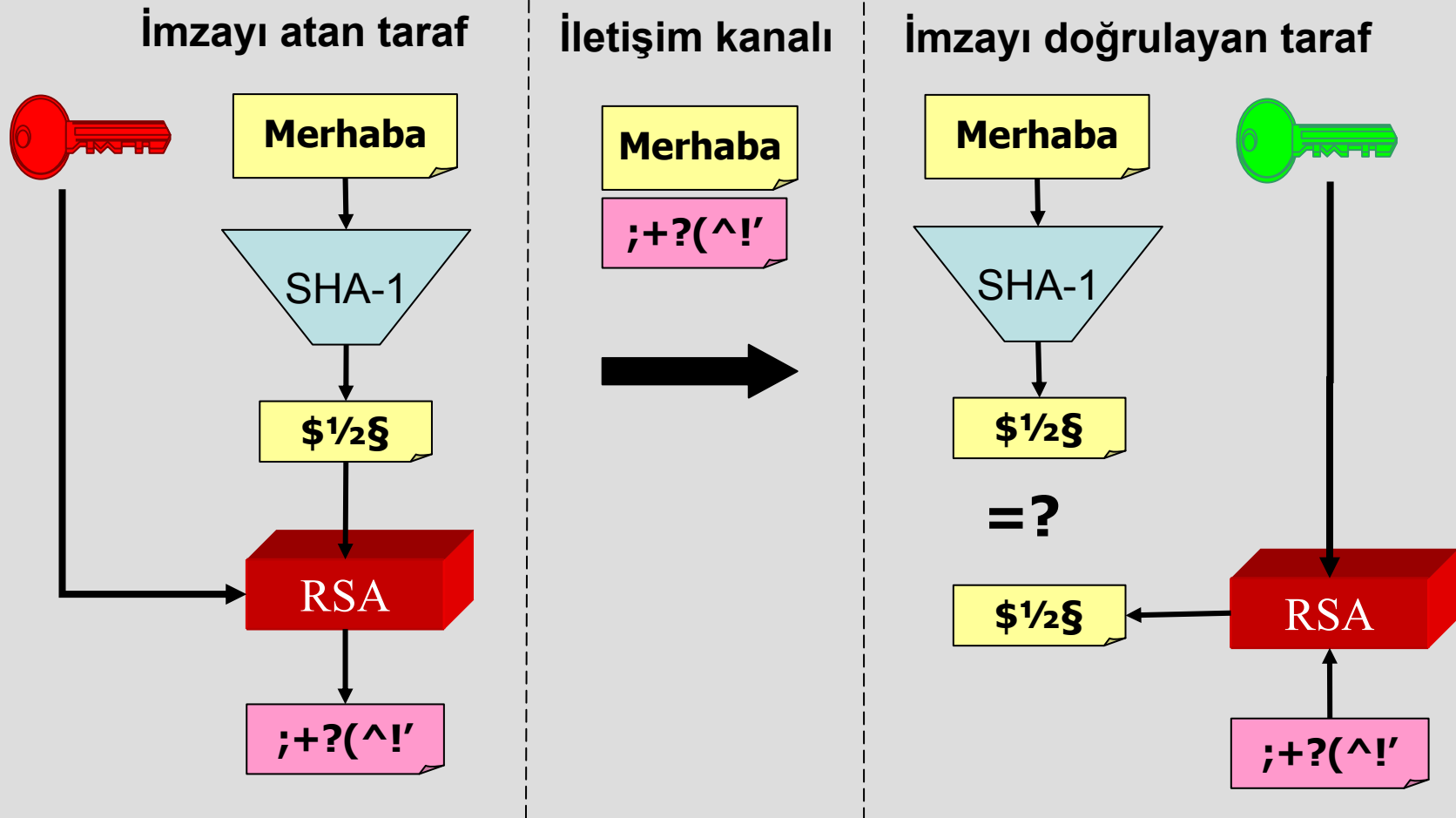
- E-imzayı oluşturmak için kullanılır.
- Sadece kişinin kendisinde bulunur.
- Güvenli elektronik imza oluşturma aracı içinde saklanır ve bu araçtan dışarıya çıkarılamaz.

Açık anahtar (imza doğrulama verisi)

“Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi veriler”

- E-imzayı doğrulamak için kullanılır.
- Gizli olmayan, herkese açık bir veridir.
- Elektronik sertifikanın içerisinde tutulur.

Elektronik İmza Mekanizması



Bilgi Bütünlüğü

Kimlik Doğrulama

İnkâr Edilemezlik

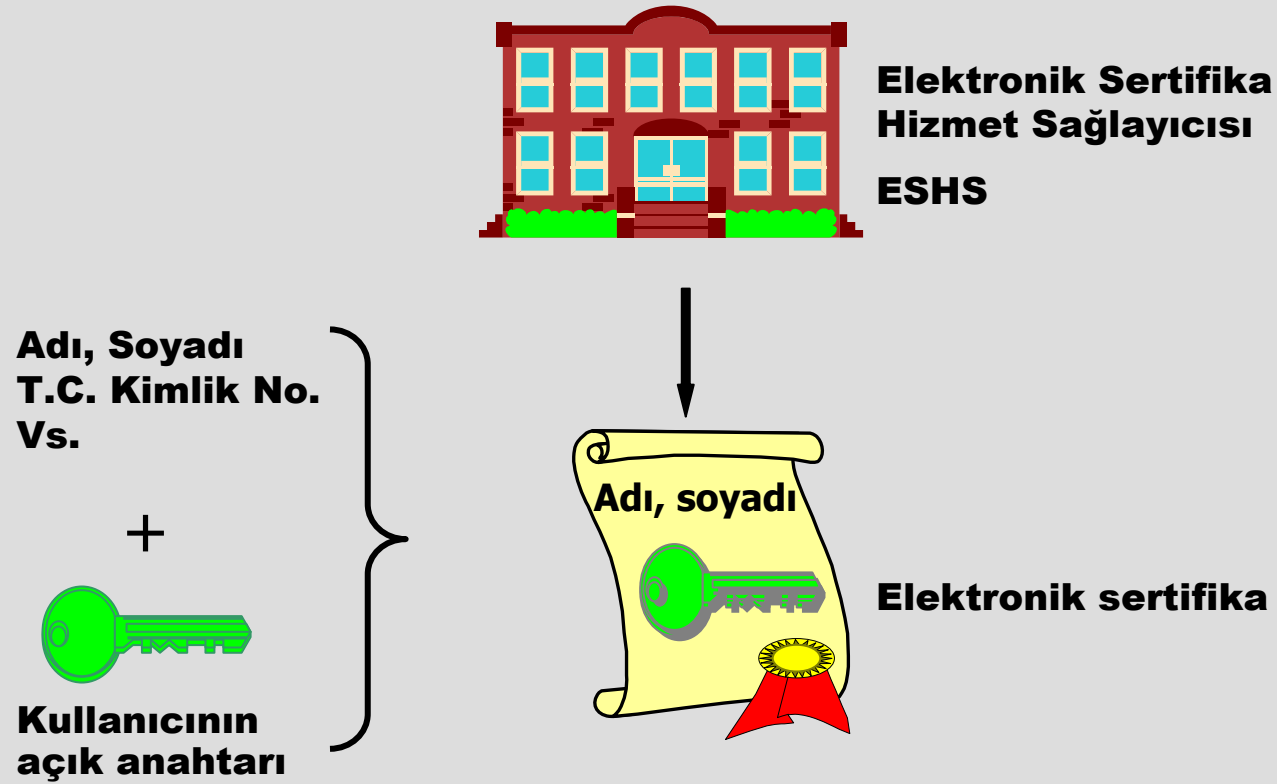
Elektronik imza



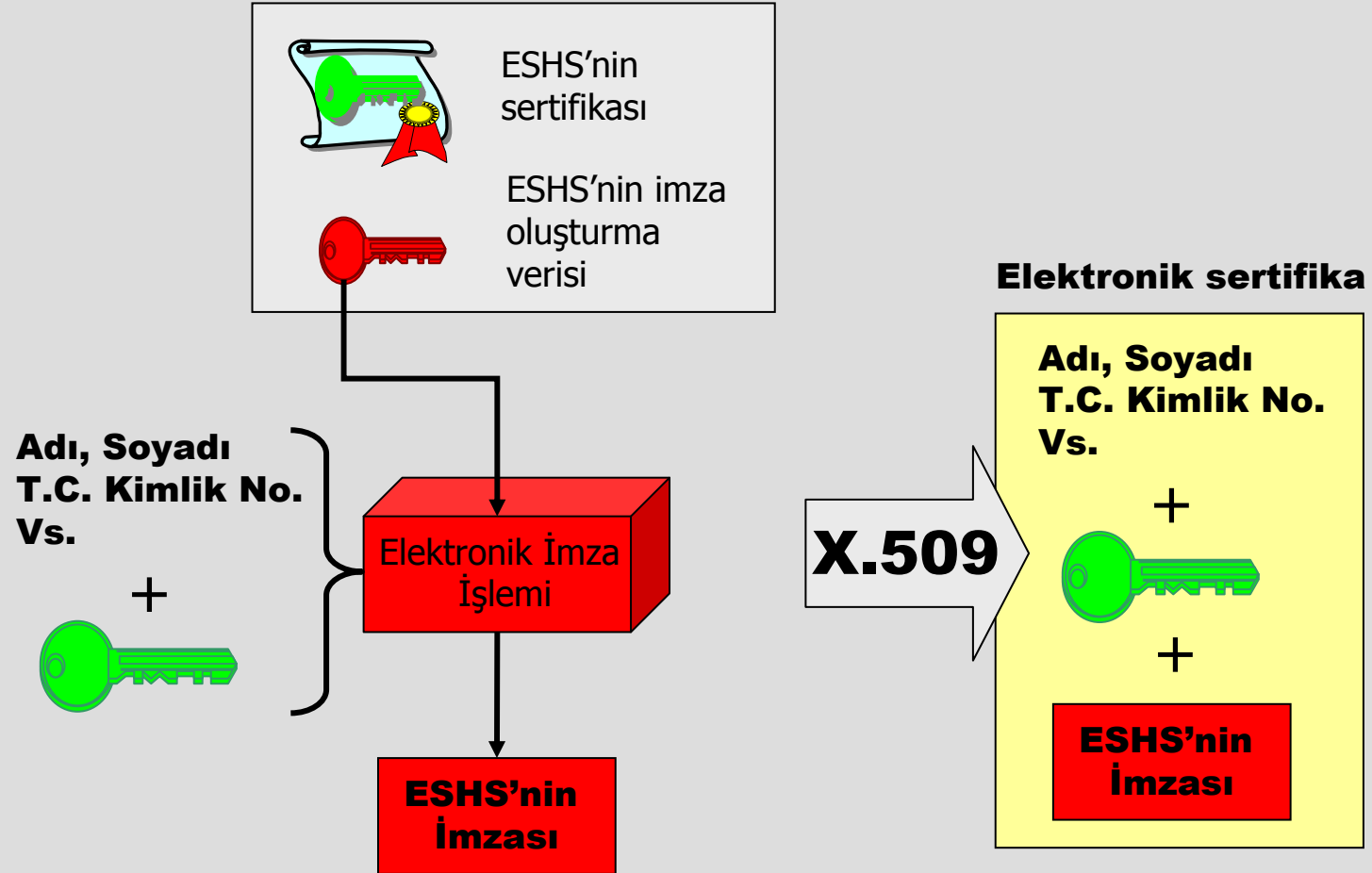
Elektronik Sertifika

Elektronik Sertifika

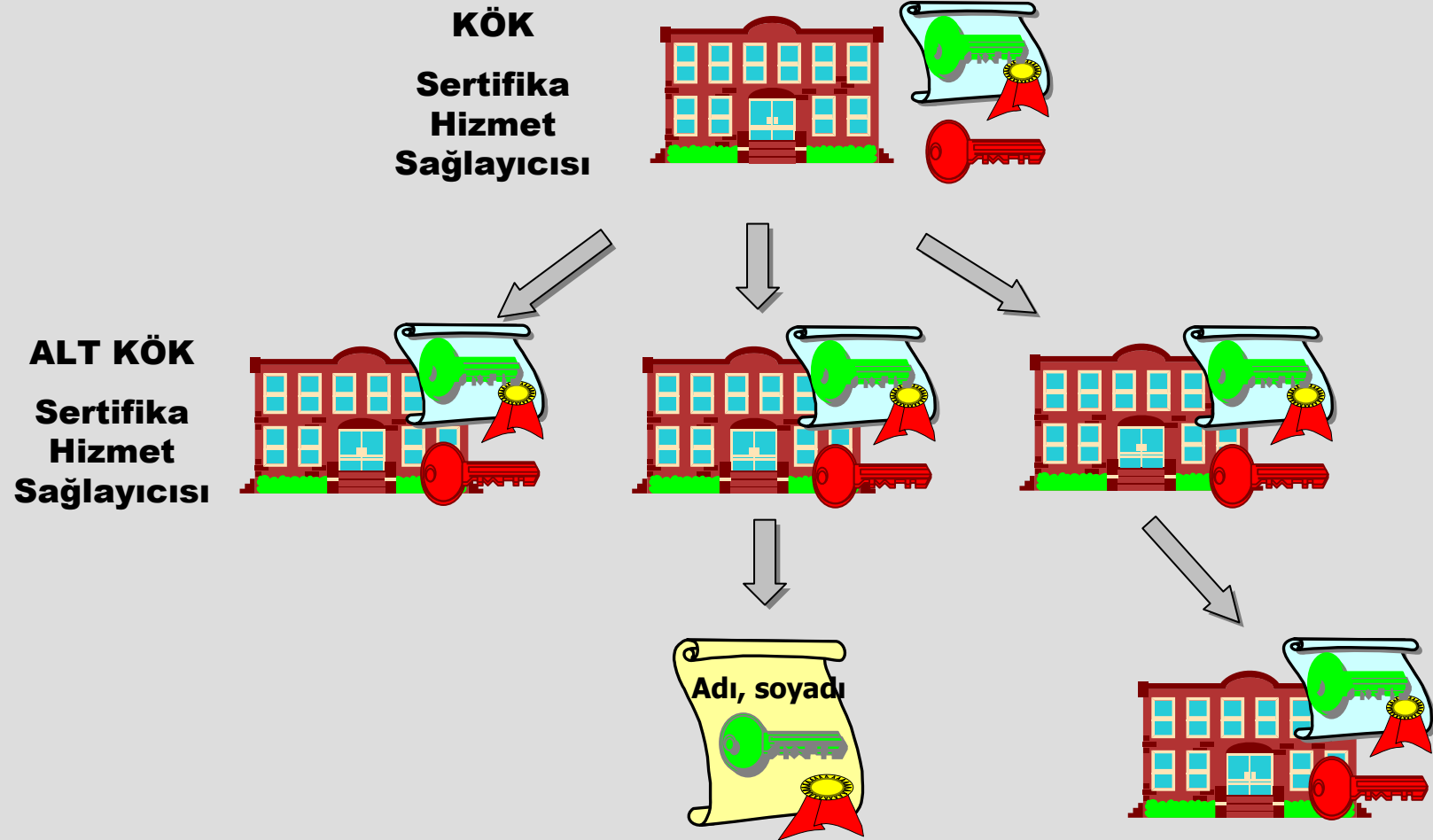
“İmza sahibinin imza doğrulama verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı”



Elektronik Sertifikanın Oluşturulması



ESHS Sertifika Güven Zinciri (Sertifika Patikası)



X.509 Elektronik Sertifika Standardı

- ITU-T X.509 Public Key and Attribute Certificate Framework
- İçerik
 - X.509 v4 Açık Anahtar Sertifikaları
(PKC Public Key Certificates)
 - Sertifika İptal Listesi v2
(CRL-Certificate Revocation List)

X.509 Sertifika İçeriği

- X.509 versiyon bilgisi
- Sertifika sahibinin isim bilgileri
- Seri numarası
- Geçerlilik süresi
- Sertifikayı veren kuruluş bilgileri
- Sertifikayı veren kuruluş erişim bilgileri
- Sertifika sahibinin açık anahtarı
- Anahtar kullanım amacı
- SiL ve OCSP erişim adresleri
- Sertifika İlkeleri erişim adresi
- Nitelikli elektronik sertifika ibareleri
- Sertifikayı veren kurumun elektronik imzası

Sertifika Veri Formatı

İkil (Binary) gösterimi

```

0 , 0 0 , 0 k 0 0 9 Ê T % $ P " 2 $ 2 Û Û û " 0 0 * † H † ÷ 0 0 0 0
S i g n ,   I n c . 1 < 0 : 0 0 U 0 0 3 C l a s s   1   P u b l i c
P r i m a r y   C e r t i f i c a t i o n   A u t h o r i t
-   G 2 1 : 0 8 0 0 U 0 0 1 ( c )   1 9 9 8   U E K A E ,   I n c .   -
F o r   a u t h o r i z e d   u s e   o n l y 1 0
0 0 0 0 U 0 0 0 T U   B I T A K   K A M U   S E R T I F I K A S Y O N
M E R K E Z İ 0 0 0 9 8 0 5 1 8 0 0 0 0 0 0 0 Z 0 1 8 0 5 1 8 2 3 5 9 5 9 Z 0
0 Á 1 0
0 0 U 0 0 0 0 U S 1 0 0 0 0 U 0 0 0 U E K A E ,   I n c . 1
< 0 : 0 0 U 0 0 3 C l a s s   1   P u b l i c   P r i m a r y
   C e r t i f i c a t i o n   A u t h o r i t y   -
G 2 1 : 0 8 0 0 U 0 0 1 ( c )   1 9 9 8   U E K A E ,   I n c .   -
F o r   a u t h o r i z e d   u s e   o n l y 1 0 0 0 0 0 U 0 0 0
N e t w o r k 0 0 Ÿ 0 0 * † H † ÷
0 0 0 0 Ğ ° ¼ 0 - , f Ô Ê Ò ¼ v 1 Ê " Ø 0
" Ė V ¼ Û o 0 o R 6 n u V U Ó ß C † ! 0 e Š ~ 0 ½ ! $ k 2
0 " 4 • 0 0 A 5 ë ' ë - İ ª Y ? 0 S m ™ O í â â * Z 0 Á ¹ Ä | 0 Ĩ È E ë | ]
0 œ > ğ d $ v ¥ Í « 0 o ¶ Ø { Q a n ! 0 † È â • â 4 Ü
A ^ ê @ ¼ s ' = k ç u 0 0 0
L Å £ j ^ ? n { ã ò 0 A f ¼ û ® ç 0 î ' ó ç 4 < ´ ² ¶ $ ò å Õ à È å b m "
{ Ě ¼ » 0 < | W Ê ğ 7 © 0 ¯ Š î 0 ¼ 0 ( œ Û & v   Í Ä 0
ğ ®
0 Õ ¼ ¯ W 0
j Ğ   B B B 0 ô   İ ¥ x , • & 8 Š G

```

Sertifika Veri Formatı

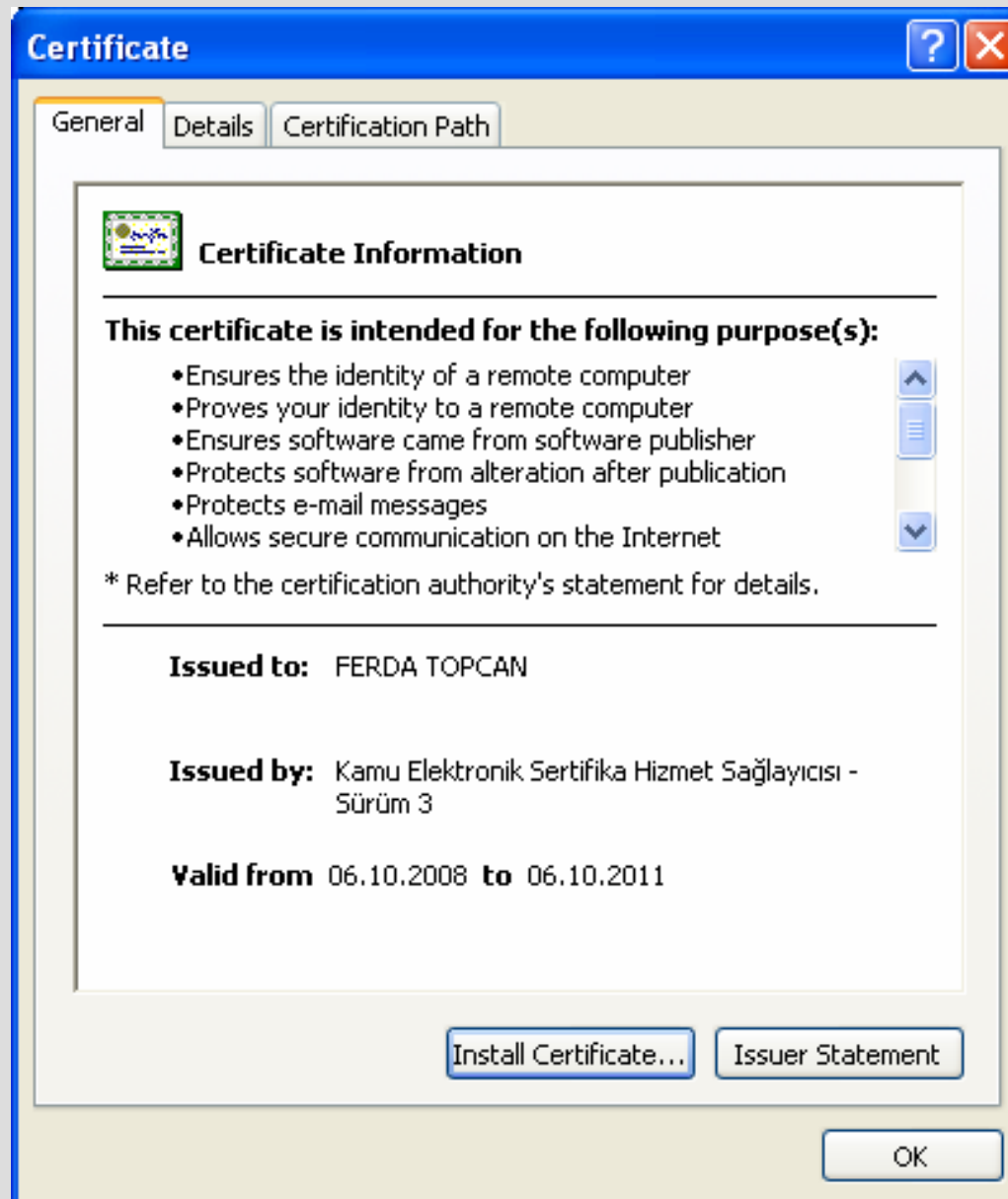
Base-64 Content Transfer Encoding

```

- - - - - B E G I N   C E R T I F I C A T E - - - - -
M I I D A j C C A m s C E D n K V I n + U C I y / j L Z 2 / s b h B k w D
B g N V B A Y T A l V T M R c w F Q Y D V Q Q K E w 5 W Z X J p U 2 l n b
c 3 M g M S B Q d W J s a W M g U H J p b W F y e S B D Z X J 0 a W Z p Y
M T o w O A Y D V Q Q L E z E o Y y k g M T k 5 O C B W Z X J p U 2 l n b
e m V k I H V z Z S B v b m x 5 M R 8 w H Q Y D V Q Q L E x Z W Z X J p U
D T k 4 M D U x O D A w M D A w M F o X D T E 4 M D U x O D I z N T k 1 O
F Q Y D V Q Q K E w 5 W Z X J p U 2 l n b i w g S W 5 j L j E 8 M D o G A
U H J p b W F y e S B D Z X J 0 a W Z p Y 2 F 0 a W 9 u I E F 1 d G h v c
Y y k g M T k 5 O C B W Z X J p U 2 l n b i w g S W 5 j L i A t I E Z v c
M R 8 w H Q Y D V Q Q L E x Z W Z X J p U 2 l n b i B U c n V z d C B O Z
A Q U A A 4 G N A D C B i Q K B g Q C q 0 L q + F i 2 4 g 9 T K 0 g + 8 d
V d P f Q 4 c h E W W K f o + 9 I d 5 r M j 8 b h D S V B Z 1 B N e u S 6
F c / I R e u m X Y 6 c P v B k J H a l z a s a b 7 b Y e 1 F h b q Z / h
A Q A B M A 0 G C S q G S I b 3 D Q E B B Q U A A 4 G B A I v 3 G h D O d
e 0 A p u X i I u k z F o 2 p e n m 5 7 4 / I C Q Q x m v q 3 7 r q I U z
v r s D i 3 x X y v A 3 q Z C v i u 4 D v h 0 o n N k m d q D N x J 1 O 8
g p U m O I p H
- - - - - E N D   C E R T I F I C A T E - - - - -

```

Elektronik Sertifika İçeriği - 1



Elektronik Sertifika İçeriği - 2

Certificate [?] [X]

General Details Certification Path

Show: <All>

Field	Value
Public key	RSA (2048 Bits)
Authority Key Identifier	KeyID=e3 87 c3 ec 1d c4 25 b7 e...
Subject Key Identifier	25 ef ce d9 38 73 01 4a 75 38 71 ...
Certificate Policies	[1]Certificate Policy:Policy Identifi...
Basic Constraints	Subject Type=End Entity, Path Le...
CRL Distribution Points	[1]CRL Distribution Point: Distribut...
Authority Information A...	[1]Authority Info Access: Access ...

30 82 01 0a 02 82 01 01 00 d5 1c 98 99 da
 46 fa a5 e8 69 53 84 3b 25 0f e6 20 8a 2f
 a5 85 2b 46 53 c7 5a 73 a4 22 9c 11 d1 ff
 76 a4 46 1b 07 6f 2d e1 c4 17 b3 27 53 0c
 90 83 27 1b ee 0e ec 62 60 90 fb ea 7c 43
 e3 12 54 52 41 ed 37 f1 c3 c8 83 0e f0 85
 07 61 15 6b 43 98 4d 28 60 bd 50 10 bd 39
 a5 25 6a 75 b2 8c 93 3b 71 4d 0e 81 a0 42
 1e 8f 85 ec ab 58 4e 5b a6 df b2 92 97 f5

Edit Properties... Copy to File...

OK

Certificate [?] [X]

General Details Certification Path

Show: <All>

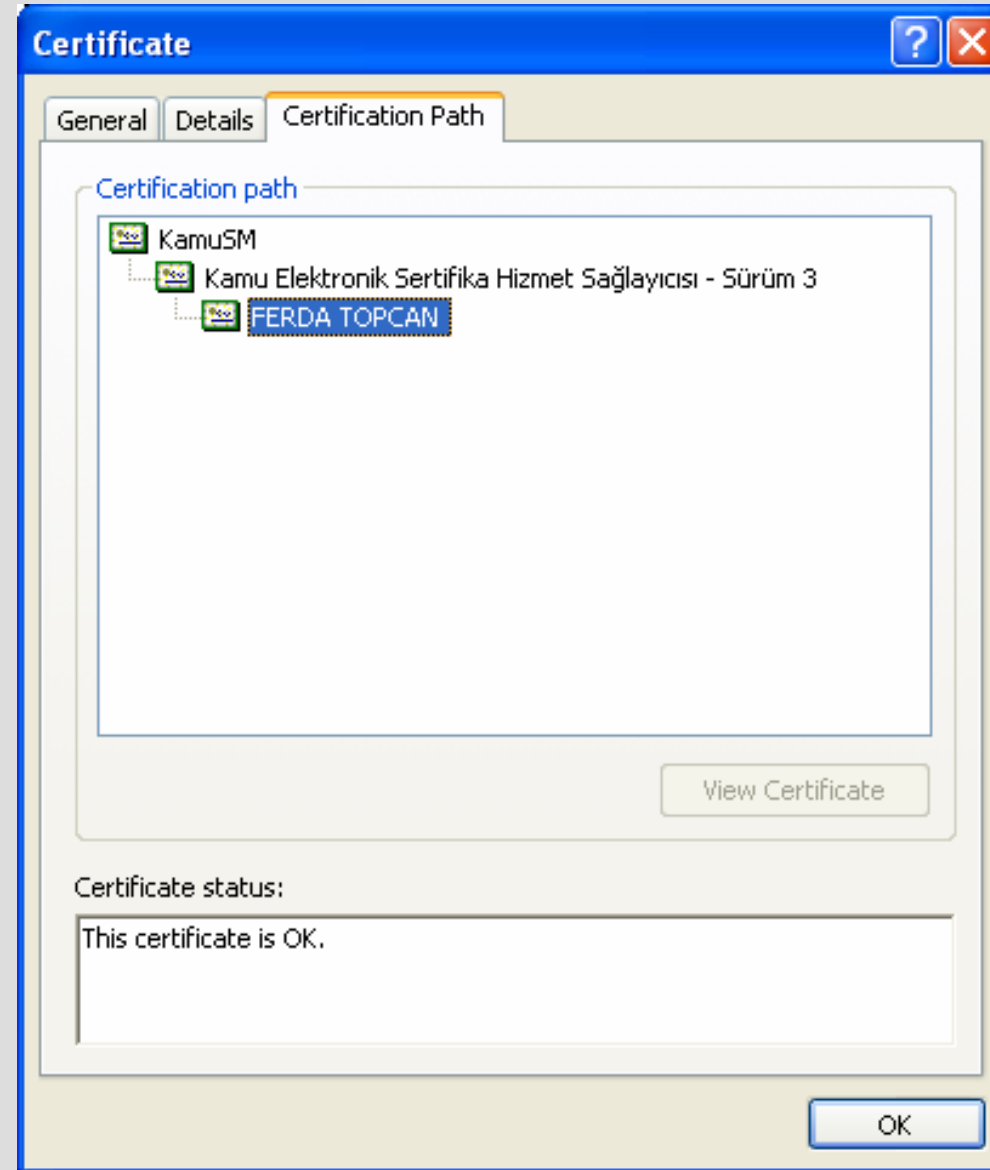
Field	Value
Public key	RSA (2048 Bits)
Authority Key Identifier	KeyID=e3 87 c3 ec 1d c4 25 b...
Subject Key Identifier	25 ef ce d9 38 73 01 4a 75 38 ...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Basic Constraints	Subject Type=End Entity, Pat...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
1.3.6.1.5.5.7.1.3	30 81 91 30 08 06 06 04 00 8e...

Qualifier:
 Notice Text=Bu sertifika, 5070 sayılı Elektronik İmza Kanununa göre nitelikli elektronik sertifikadır.

Edit Properties... Copy to File...

OK

Elektronik Sertifika İçeriği - 3



Elektronik Sertifika Yönetimi

Anahtarların Üretimi

- Güvenilir ortamlarda, güvenlik şartlarına uygun yazılımlar veya donanım araçları içinde üretilir.
- Kullanıcı adına ESHS'ler tarafından üretilir.
- Kullanıcı tarafından üretilebilir. Bu durumda aşağıdaki şartın sağlanması gereklidir:

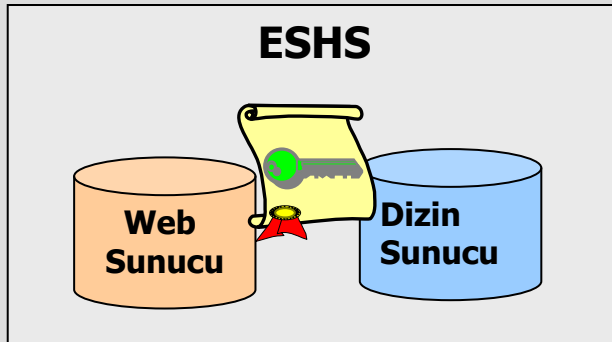
Açık anahtara karşılık gelen özel anahtarın varlığının kriptolojik yöntemler kullanılarak doğrulanması yoluyla, açık anahtarın geçerli bir anahtar olduğu ESHS tarafından kontrol edilmelidir.



Elektronik Sertifika Yönetimi

Anahtarların Bulunduğu Ortamlar

- Özel anahtar güvenli elektronik imza oluşturma aracı içinde PIN erişimli bölümde şifreli olarak saklanır.
- Açık anahtar elektronik sertifika içinde, elektronik sertifikalar ise herkesin erişebileceği ortamlarda bulundurulur. Örn: ESHS'lere ait sunucular.
- Elektronik sertifikaya imza sahibine ait güvenli elektronik imza oluşturma aracı ve imzalı verinin içeriginden de erişilebilir.



Elektronik Sertifika Yönetimi

Anahtarların Kullanım Amaçları

- Özel anahtar: Güvenli elektronik imza oluşturma amacıyla kullanılır. Başka bir amaç için kullanılmaz.
- Açık anahtar: Oluşturulan güvenli elektronik imzanın doğrulanması için kullanılır. Başka bir amaç için kullanılmaz.

Elektronik Sertifikanın Geçerlilik Süresi

- Anahtarların kriptografik açıdan güvenlik süresi:
 - 1024-bit : 1 yıl
 - 2048-bit : 6-10 yıl
- Elektronik sertifika sahibinin kimliğinin geçerlilik süresi

Geçerlilik süresi dolan elektronik sertifikaya ait özel anahtar imza oluşturma amaçlı kullanılmaz. Açık anahtar geçmişte oluşturulmuş imzaların doğrulanması için kullanılır.

Elektronik Sertifika Yönetimi

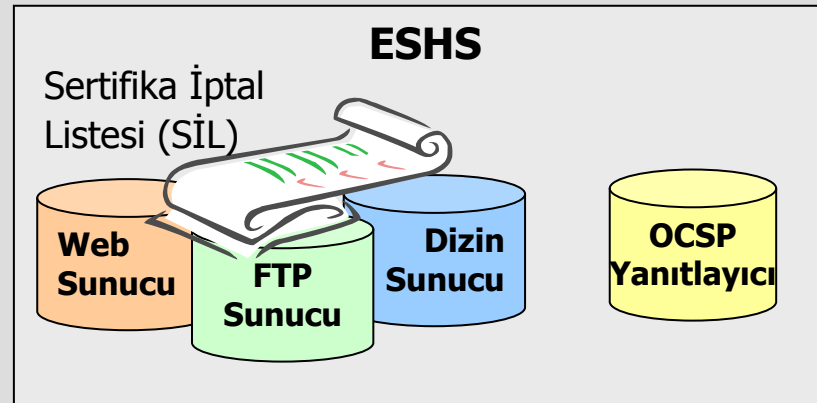
Elektronik Sertifikanın Yenilenmesi

- Elektronik sertifikanın geçerlilik süresi dolduğunda (veya dolmasına yakın bir süre önce) ESHS'ye başvurulur ve kullanıcıya yeni bir sertifika üretilir.
- Yenilemede imza sahibine yeni anahtar çiftleri üretilir.
- Eski özel anahtar, sahibi tarafından imha edilmelidir.
- Eski sertifika, geçmişte oluşturulmuş e-imzaların doğrulanması amaçlı arşivlenir.

Elektronik Sertifika Yönetimi

Elektronik Sertifikanın İptal Edilmesi


- Geçerlilik süresi dolmadan özel anahtarın kullanımı engellenebilir.
- Özel anahtarın kullanımının engellendiği sertifikanın iptal edilmesi ile duyurulur.
- Sertifikanın iptal edildiği sertifikayı veren ESHS tarafından duyurulur.
 - Sertifika İptal Listesi (SİL)
 - OCSP (*Online Certificate Status Protocol* - Çevrimiçi Sertifika Durum Protokolü)



Sertifika İptal Listesi - 1

Certificate Revocation List [?] [X]

General | Revocation List

 **Certificate Revocation List Information**

Field	Value
Version	V2
Issuer	Kamu Elektronik Sertifika Hizmet S...
Effective date	22 Aralık 2009 Salı 10:26:21
Next update	23 Aralık 2009 Çarşamba 22:27:20
Signature algorithm	sha1RSA
CRL Number	51836
Authority Key Iden...	KeyID=e3 87 c3 ec 1d c4 25 b7 ed...

Value:

CN = Kamu Elektronik Sertifika Hizmet Sağlayıcısı - Sürüm 3
OU = Kamu Sertifikasyon Merkezi
OU = Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü - UEKAE
O = Türkiye Bilimsel ve Teknolojik Araştırma Kurumu - TÜBİTAK
L = Gebze - Kocaeli
C = TR

OK

Sertifika İptal Listesi - 2

Certificate Revocation List [?] [X]

General | Revocation List

Revoked certificates:

Serial number	Revocation date
1a b8	05 Eylül 2007 Çarşamba 07:55:53
1a c1	18 Ocak 2008 Cuma 09:05:47
1a f2	24 Kasım 2008 Pazartesi 09:42:01
1b 2c	23 Kasım 2007 Cuma 08:01:37
1b 02	01 Şubat 2008 Cuma 09:30:46
1h 33	23 Kasım 2007 Cuma 07:58:15

Revocation entry

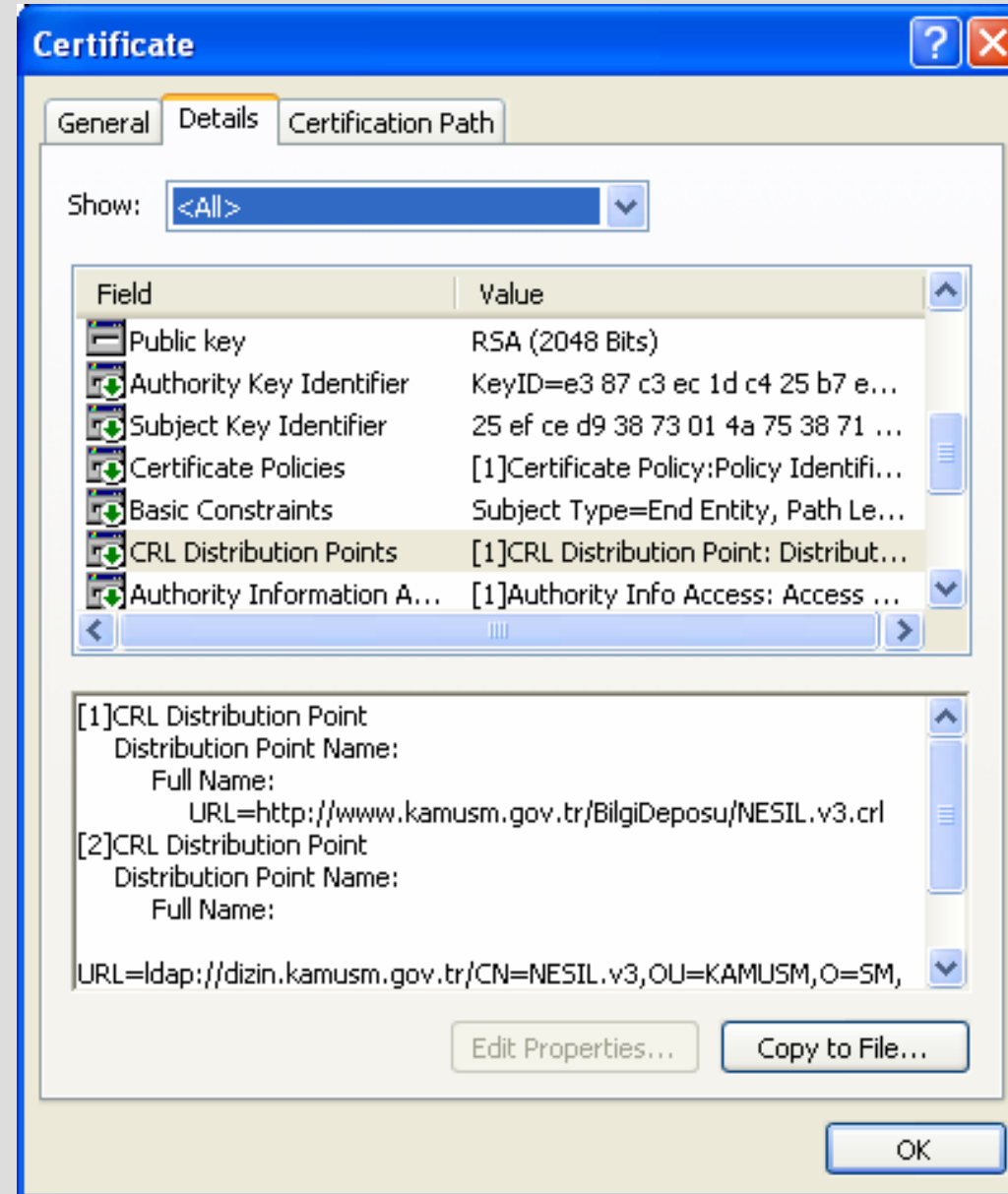
Field	Value
Serial number	1b 02
Revocation date	01 Şubat 2008 Cuma 09:30:46

Value:

01 Şubat 2008 Cuma 09:30:46

OK

Sertifika İçeriğindeki SİL Dağıtım Noktası Bilgisi



OCSP (Online Sertifika Durum Protokolü)

<http://ocsp3.kamusm.gov.tr>

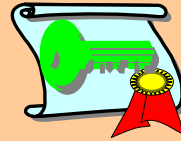
**İMZA
OLUŞTURMA
VEYA
DOĞRULAMA
UYGULAMASI**



Sertifika seri numarası



Sertifika geçerli



OCSP İMZASI

OCSP Cevabı

Sorgulama sonucu:

- Sertifika geçerli
- Sertifika iptal olmuş
- Bilinmiyor

Sertifika İçeriğindeki OCSP Erişim Bilgisi

