BİLGİ VE BİLGİSAYAR GÜVENLİĞİ DERSİ
ARAŞTIRMA PROJESİ

SAYISAL (ELEKTRONİK) İMZA VE AÇIK ANAHTAR ALTYAPISI

HÜSEYİN EROL
BİLGİSAYAR MÜH. YÜKSEK LİSANS
24290361
ARALIK 2004 ANKARA

Takdim Planı

- Giriş
- Temel Kavramlar
- Sayısal (Elektronik) İmza
- Açık Anahtar Altyapısı ile Sayısal İmza Çözümü
- Açık Anahtar Altyapısı Bileşenleri
- Açık Anahtar Altyapısı Mimarileri
- Sonuç

Giriş

Bu çalışmada, artık günümüzde hızla kullanım alanı genişleyen ve sayısal imza kanununun da çıkmasıyla resmiyet kazanan sayısal (elektronik) imza konusu incelenmiştir. Ülkemizde hukuki ve teknik yönleri 15 Ocak 2004 tarihinde TBMM Genel Kurulunda kabul edilip yasalaşan ve 23 Ocak 2004 tarihinde 25355 sayılı Resmi gazetede yayımlanmış olan sayısal imza kavramının net olarak anlaşılmasını sağlamak için ülkemizde de kurulum çalışmaları devam eden Açık Anahtar Altyapısı ile sayısal imza çözümü detaylı olarak anlatılmıştır.

Takdim Planı

- Giriş
- Temel Kavramlar
- Sayısal (Elektronik) İmza
- Açık Anahtar Altyapısı ile Sayısal İmza Çözümü
- Açık Anahtar Altyapısı Bileşenleri
- Açık Anahtar Altyapısı Mimarileri
- Sonuç

Temel Kavramları

- Kriptoloji
- Haberleşme emniyeti ve Çözümleri
  - Elektronik Tehditler
  - Elektronik Tedbirler
  - Elektronik Emniyet Yöntemlerinin Karşılaştırılması
- Şifreleme Yöntemleri
  - Simetrik (Gizli Anahtarlı) Şifreleme
  - Asimetrik (Açık Anahtarlı) Şifreleme

Kriptoloji

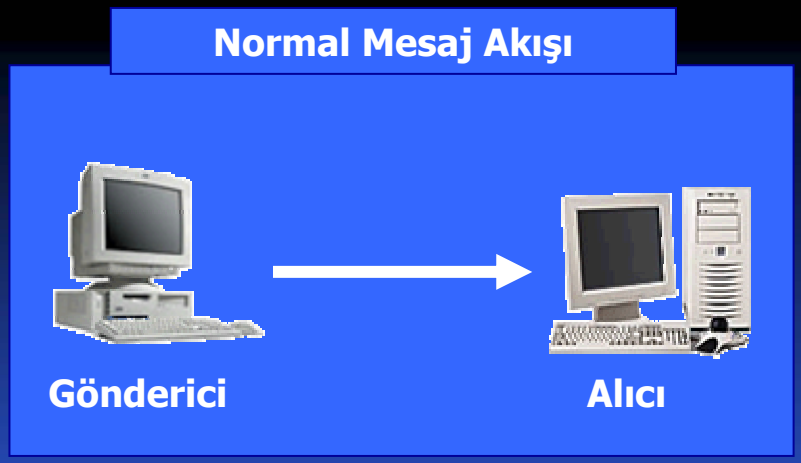
- Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür.
- Kriptografi, belgelerin şifrelenmesi ve şifrenin çözülmesi için kullanılan yöntemlere verilen addır.
- Kriptoanaliz ise; kriptografi sistemleri tarafından ortaya konan bir şifreleme sistemini inceleyerek zayıf ve kuvvetli yönlerini ortaya koymayı amaçlayan bilim dalıdır.

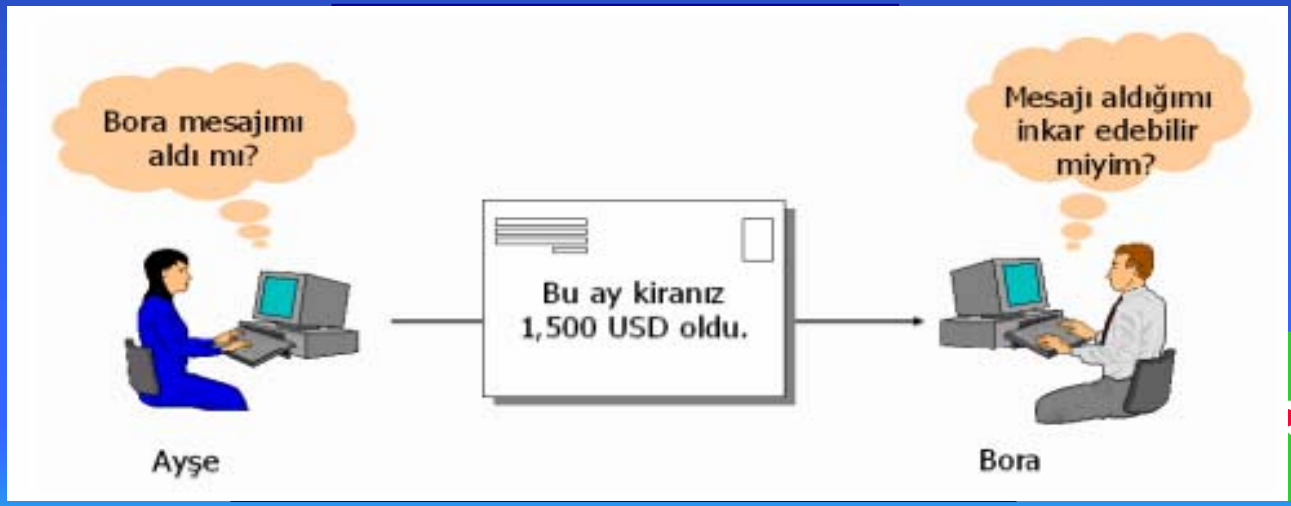
Haberleşmede Emniyet Öğeleri

- Gizlilik (Confidentiality)
- Mesaj Bütünlüğü (Integrity)
- Gönderici Kimliğini Doğrulama (Authentication)
- İnkâr Edememezlik (Non-repudiation)

ve Haberleşmenin Sürekliliği

Elektronik Tehditler





Elektronik Haberleşme Emniyeti Çözümleri

Gizlilik	Veri şifreleme
Bütünlük	Sayısal İmzalama, Sertifikalar, Kimlikler
Kimlik Doğrulaması	Özetleme Algoritmaları, Mesaj Özetleri, Sayısal İmzalar
İnkâr Edememezlik	Sayısal İmzalama, İşlem Kayıtları
Süreklilik	Yedek Sistemler, Bakım, Yedekleme

Elektronik Emniyet Yöntemlerinin Karşılaştırılması

	Kimlik Kanıtlama	Gizlilik	Bütünlük	İnkâr Edememe
Anti-virüs			✓	
Güvenlik Duvarları	✓	✓		
Erişim Denetimi	✓	✓		
Şifreleme		✓		
Sayısal İmza	✓		✓	✓
Açık Anahtar Altyapısı	✓	✓	✓	✓

Şifreleme (Kriptoloji) Nedir?

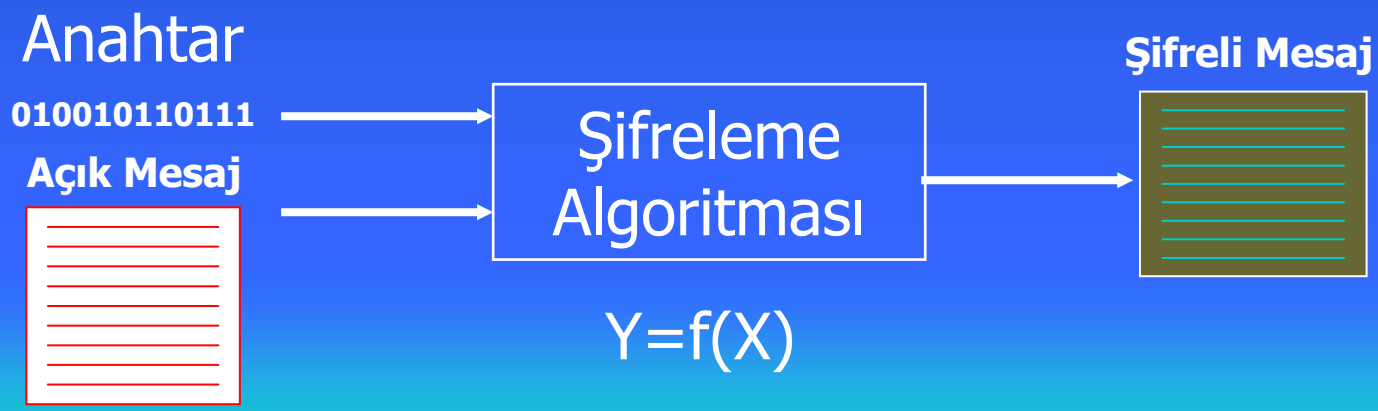
Şifreleme, kritik bir bilginin gizliliğinin güvensiz ortamlarda sürdürülmesi amacıyla yapılan işlemler bütününe verilen isimdir.

Güvenli Şifreleme Yöntemleri

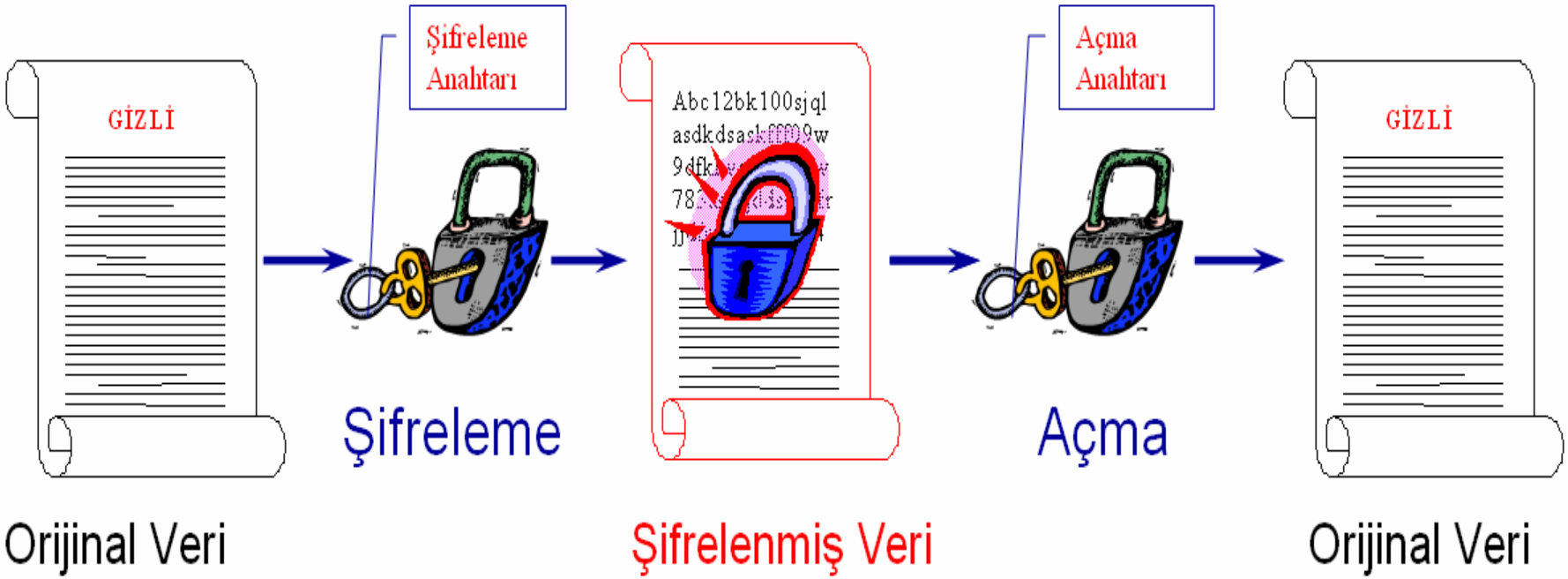
- 64 bitlik bir anahtar = 

1100101010110001
0001101000000111
0110100010011110
1100111010011011

- 64 bitlik bir anahtarı tahmin yoluyla elde etme olasılığı $1/2^{64} = 1/10^{19}$



Güvenli Şifreleme Algoritmaları

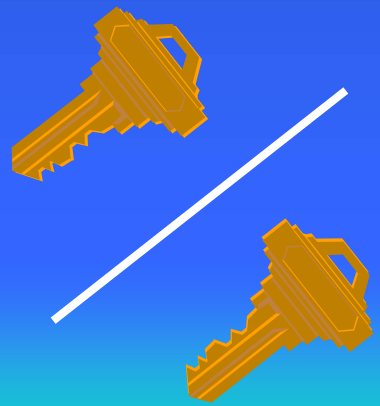


Şifreleme ve açma işlemlerinde kullanılan anahtarların birbiriyle olan ilişkilerine bağlı olarak, iki tür şifreleme algoritması vardır:

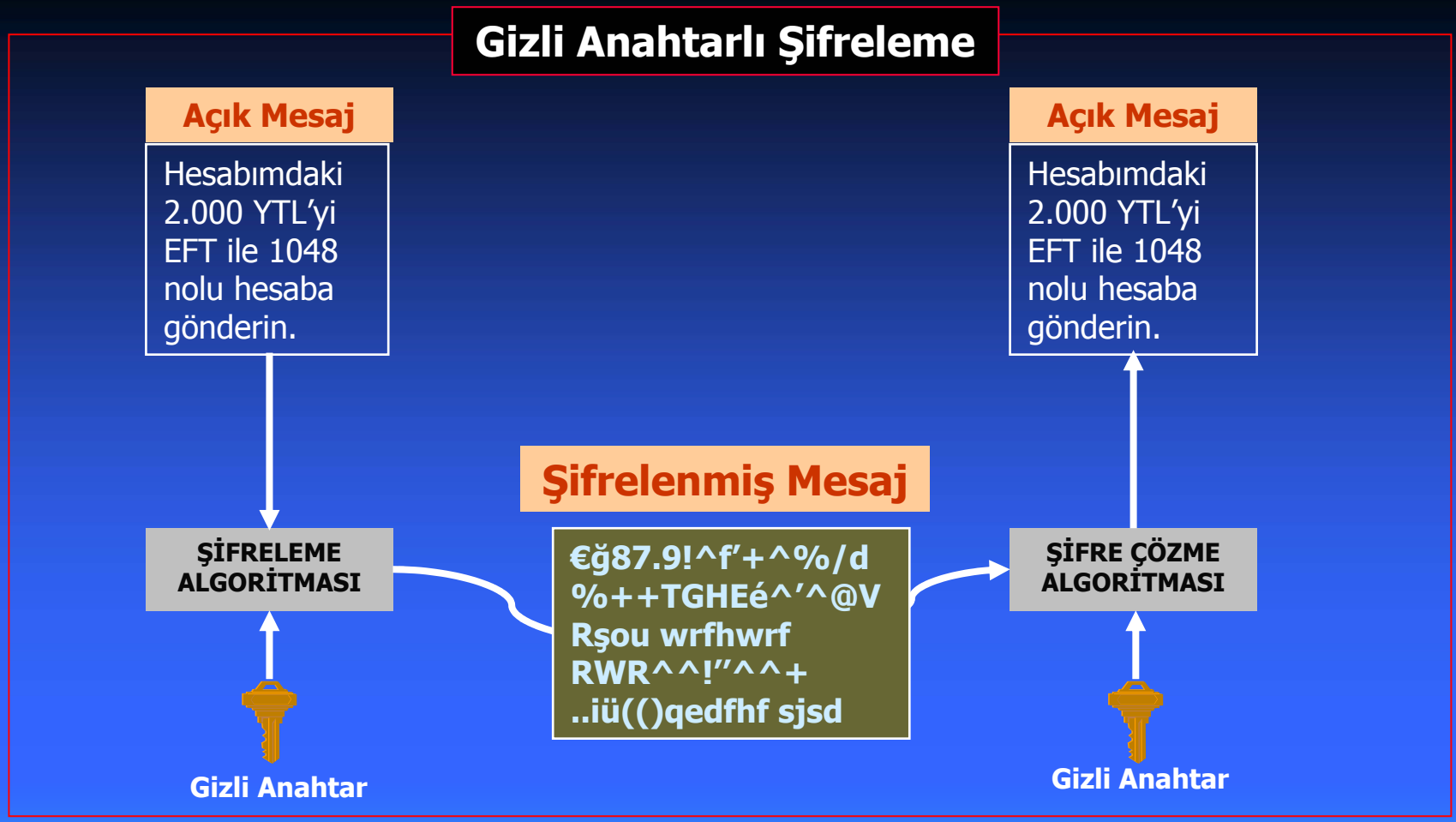
- *Simetrik (Gizli Anahtarlı) Şifreleme Algoritmaları*
- *Asimetrik (Açık Anahtarlı) Şifreleme Algoritmaları*

Simetrik (Gizli Anahtarlı) Şifreleme

- Simetrik şifreleme algoritmaları, şifreleme ve açma işlemleri için aynı anahtarı kullanır.
- Gizli veri alışverişi yapacak kişi veya uygulamalar simetrik anahtarı kendi aralarında, emniyetli bir şekilde, değiştirmelidir.
- Simetrik şifreleme algoritmasıyla şifrelenmiş bir verinin güvenliği, şifreleme işleminde kullanılmış olan anahtarın gizliliği ile doğrudan ilişkilidir.

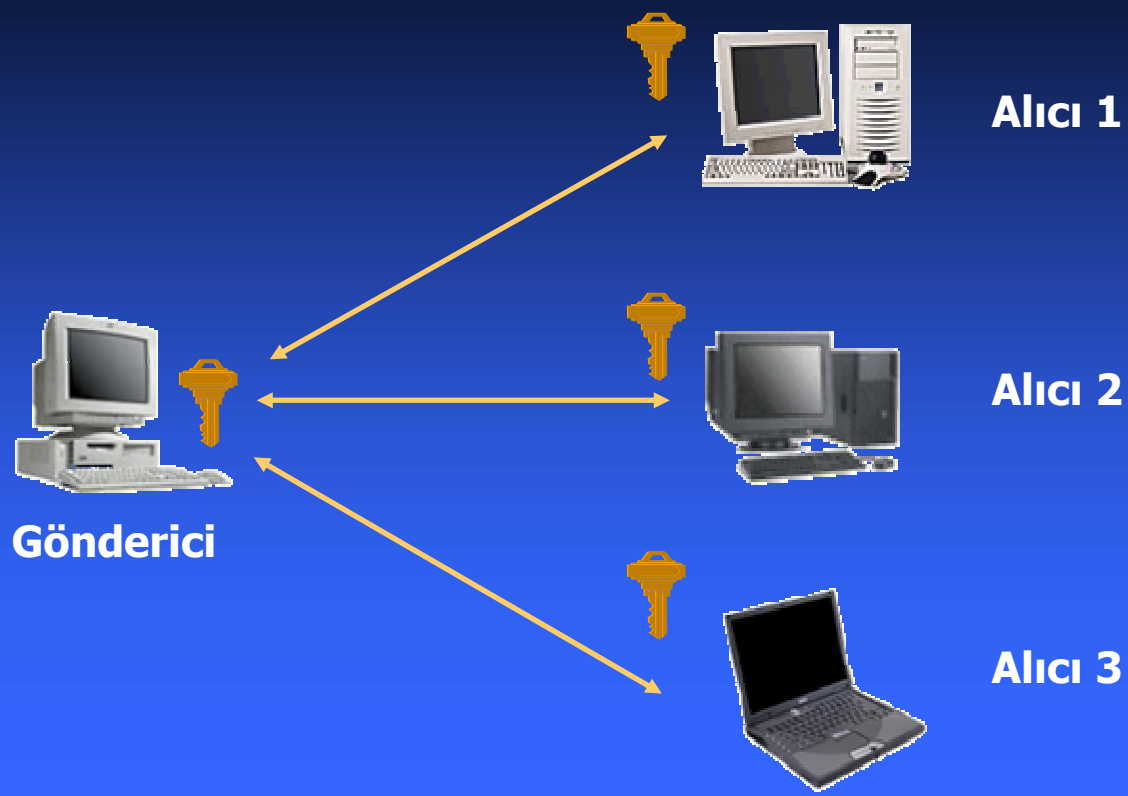


Simetrik (Gizli Anahtarlı) Şifreleme



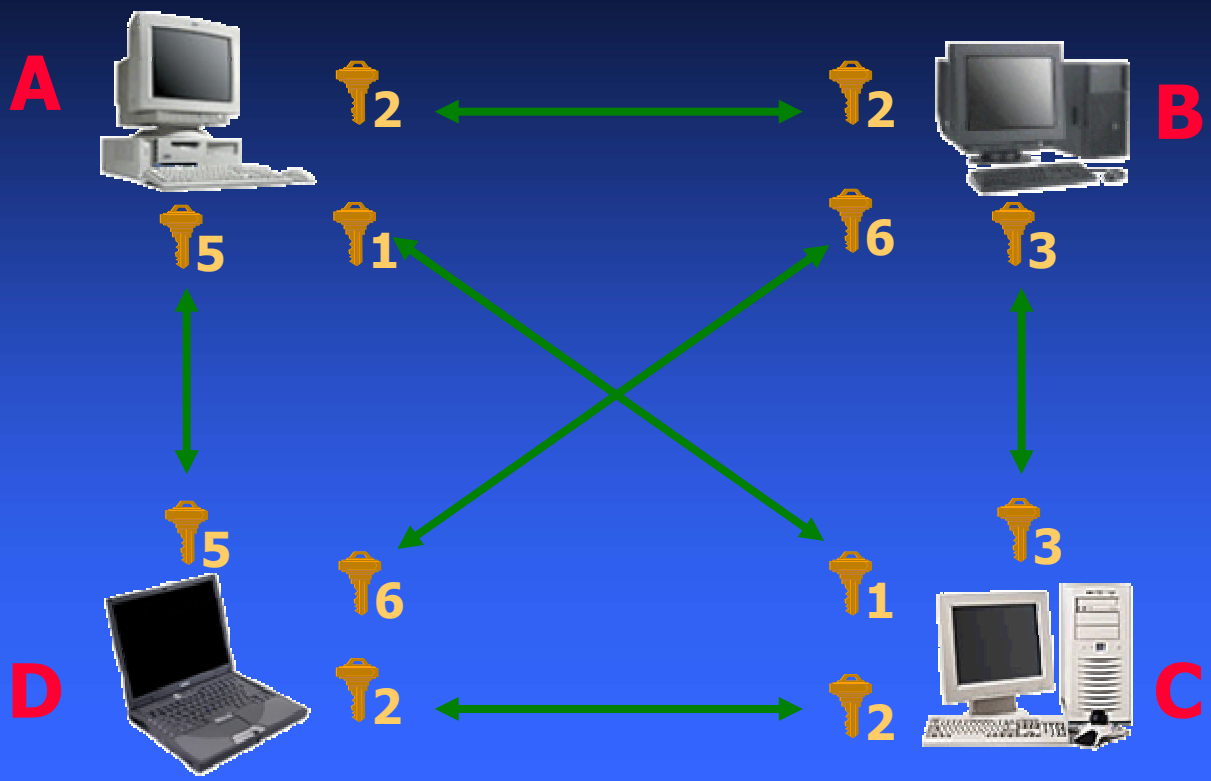
Simetrik Şifreleme Anahtar Yönetimi

Birden-Çoğa (One-to-Many)



Simetrik Şifreleme Anahtar Yönetimi

Çoktan-Çoğa (Many-to-Many)



Kullanıcı Sayısı	Anahtar Sayısı
3	3
4	6
10	45
100	4,950
1,000	499,500
10,000	49,995,000
	!!!?

Simetrik Şifrelemenin Artıları ve Eksileri

- Artılar ☺
  - Algoritmalar hızlıdır
  - Algoritmaların donanımla gerçeklenmesi kolaydır
  - “Gizlilik” güvenlik hizmetini yerine getirir
- Eksiler ☹
  - Ölçeklenebilir değil
  - Emniyetli anahtar dağıtımı zor
  - “Bütünlük” ve “Kimlik Doğrulama” güvenlik hizmetlerini gerçeklemek zor
  - Sayısal imza desteği yok!

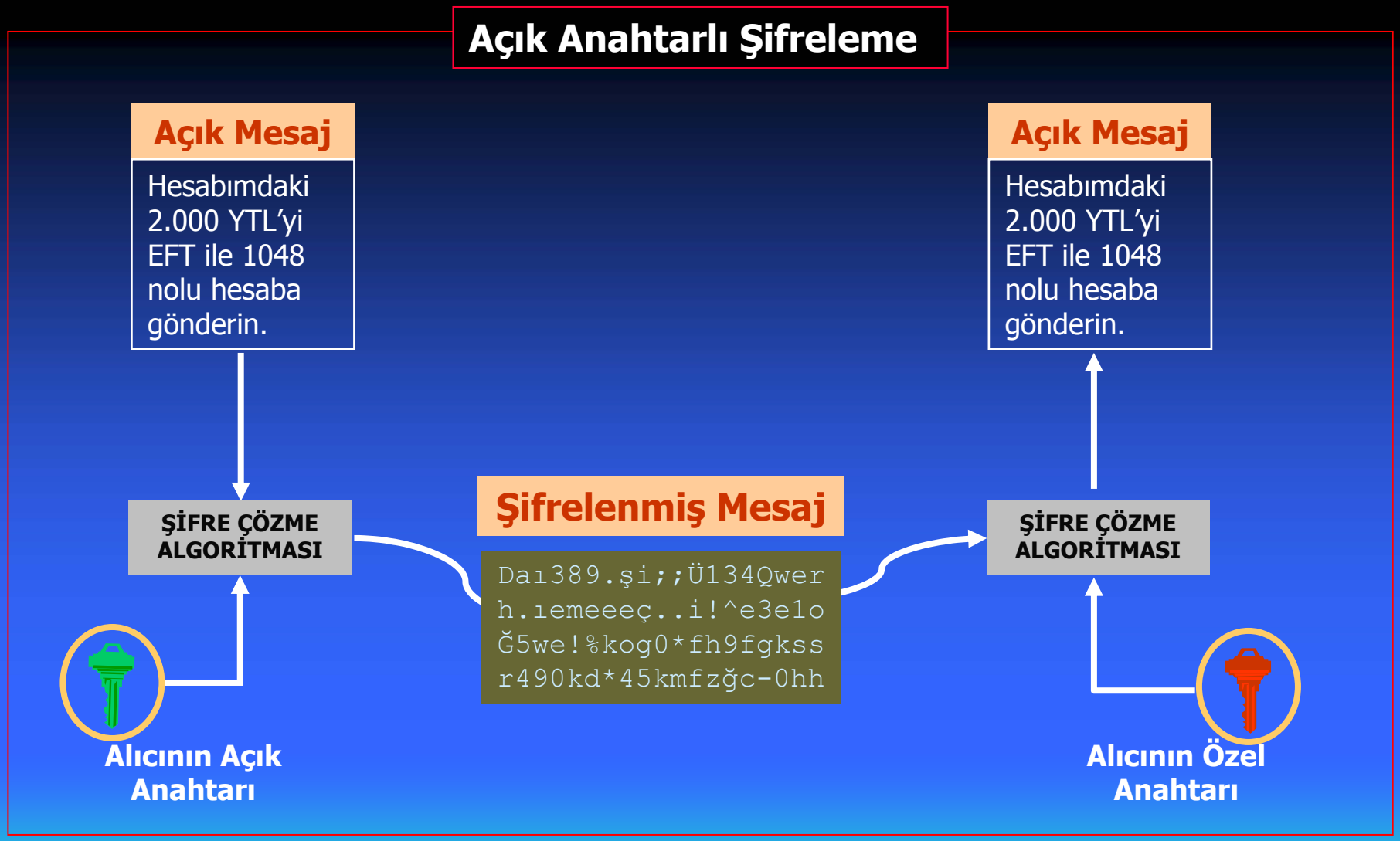
Simetrik Şifreleme Algoritmaları

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algotirhm)
- Skipjack
- RC5
- RC2
- RC4

Asimetrik (Açık Anahtarlı) Şifreleme

- Asimetrik 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.

Asimetrik (Açık Anahtarlı) Şifreleme



Asimetrik Şifreleme Anahtar Yönetimi

- Açık anahtarlar yayınlanmalı ve değiştirilmeleri önlenmelidir
- Anahtar çiftleri merkezi bir otorite tarafından üretilebilir veya her kullanıcı kendi anahtar çiftini üretebilir
- Şifreleme ve İmzalama için ayrı ayrı anahtar çiftleri olabilir (olmalıdır!)
- Anahtar iptalleri kontrollü olmalıdır.
- 10,000 kullanıcı = 10,000 anahtar çifti

Asimetrik Şifrelemenin Artıları ve Eksileri

- Artılar ☺
  - Anahtar yönetimi ölçeklenebilir
  - Kripto-analize karşı dirençli (Kırılması zor)
  - Bütünlük, Kimlik Doğrulama ve İnkâr Edememezlik güvenlik hizmetleri sağlanabilir
  - Sayısal imza desteği!
- Eksiler ☹
  - Algoritmalar genel olarak yavaş (Simetrik kriptografi algoritmalarına göre ~1500 kat!)
  - Anahtar uzunluğu bazı durumlar için kullanışlı değil

Asimetrik Şifreleme Algoritmaları

- RSA (Rivest-Shamir-Adleman)
- El Gamal
- PGP (Pretty Good Privacy)
- Diffie-Hellman anahtar belirleme
- DSA (Digital Signature Algorithm)

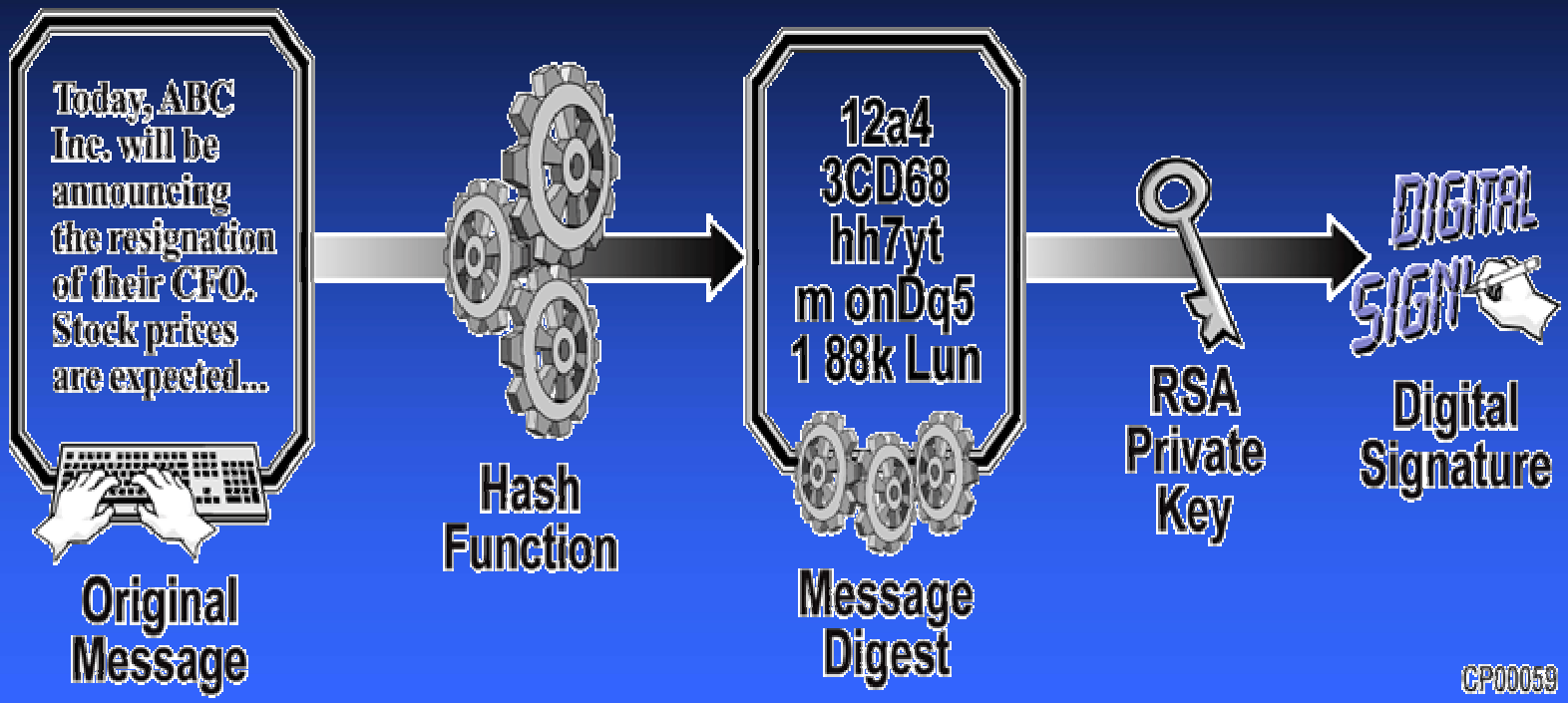
Takdim Planı

- Giriş
- Temel Kavramlar
- Sayısal (Elektronik) İmza
- Açık Anahtar Altyapısı ile Sayısal İmza Çözümü
- Açık Anahtar Altyapısı Bileşenleri
- Açık Anahtar Altyapısı Mimarileri
- Sonuç

Sayısal (Elektronik) İmza

- Sayısal (Elektronik) İmza
- Sayısal (Elektronik) İmza Nasıl Çalışır?
- Mesaj Özeti
- Açık Anahtar Altyapısı Neden Gereklidir?

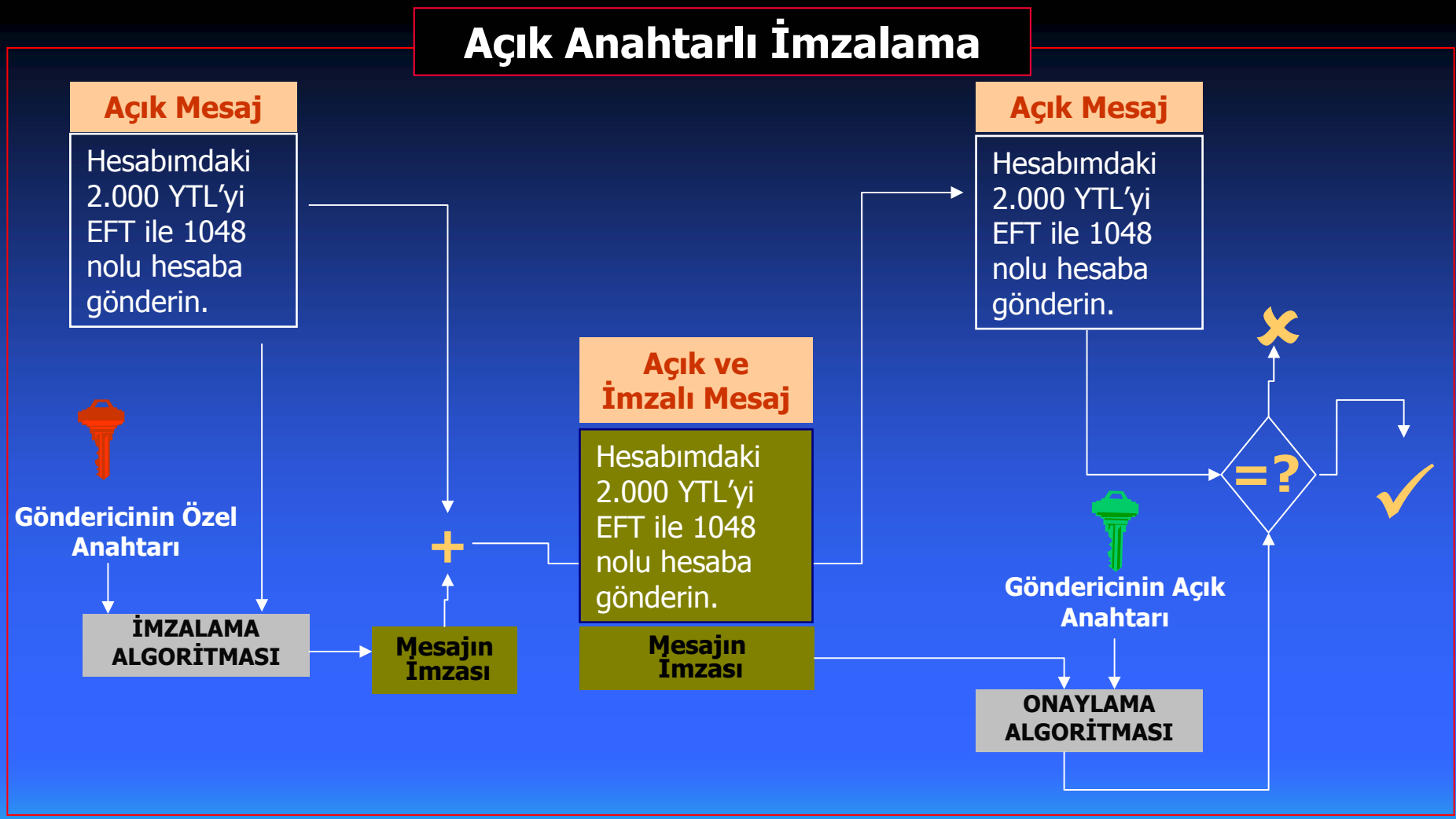
Sayısal (Elektronik) İmza



Sayısal (Elektronik) İmza

- Kriptografik dönüşümdür
- Mesajın sonuna eklenir
- Mesaj alıcısının, mesajın göndericisinin kimliğini doğrulamasını ve mesajın bütünlüğünü kontrolünü sağlar
- İnkâr edememezlik hizmetini sağlar
- Asimetrik kriptografi kullanır

Sayısal (Elektronik) İmza Nasıl Çalışır?



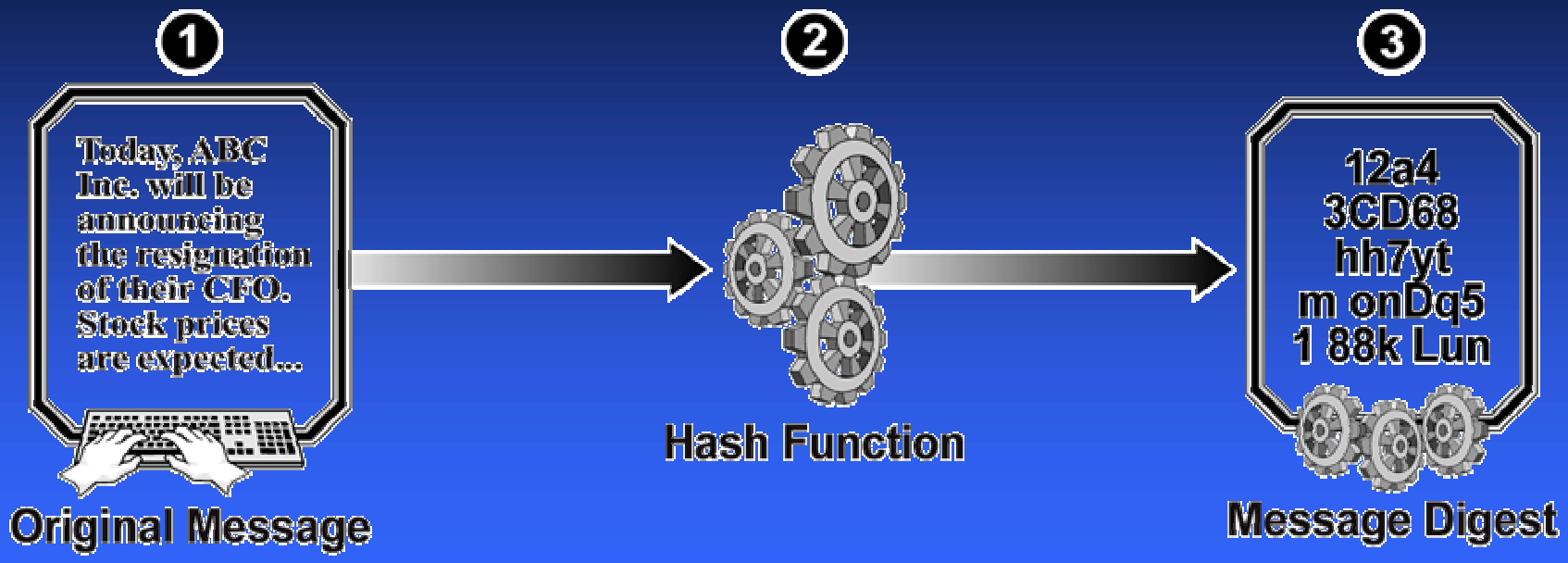
Sayısal İmza ve Özetleme Fonksiyonu

Problem: Sayısal imza mesaj uzunluğunu iki katına çıkarır

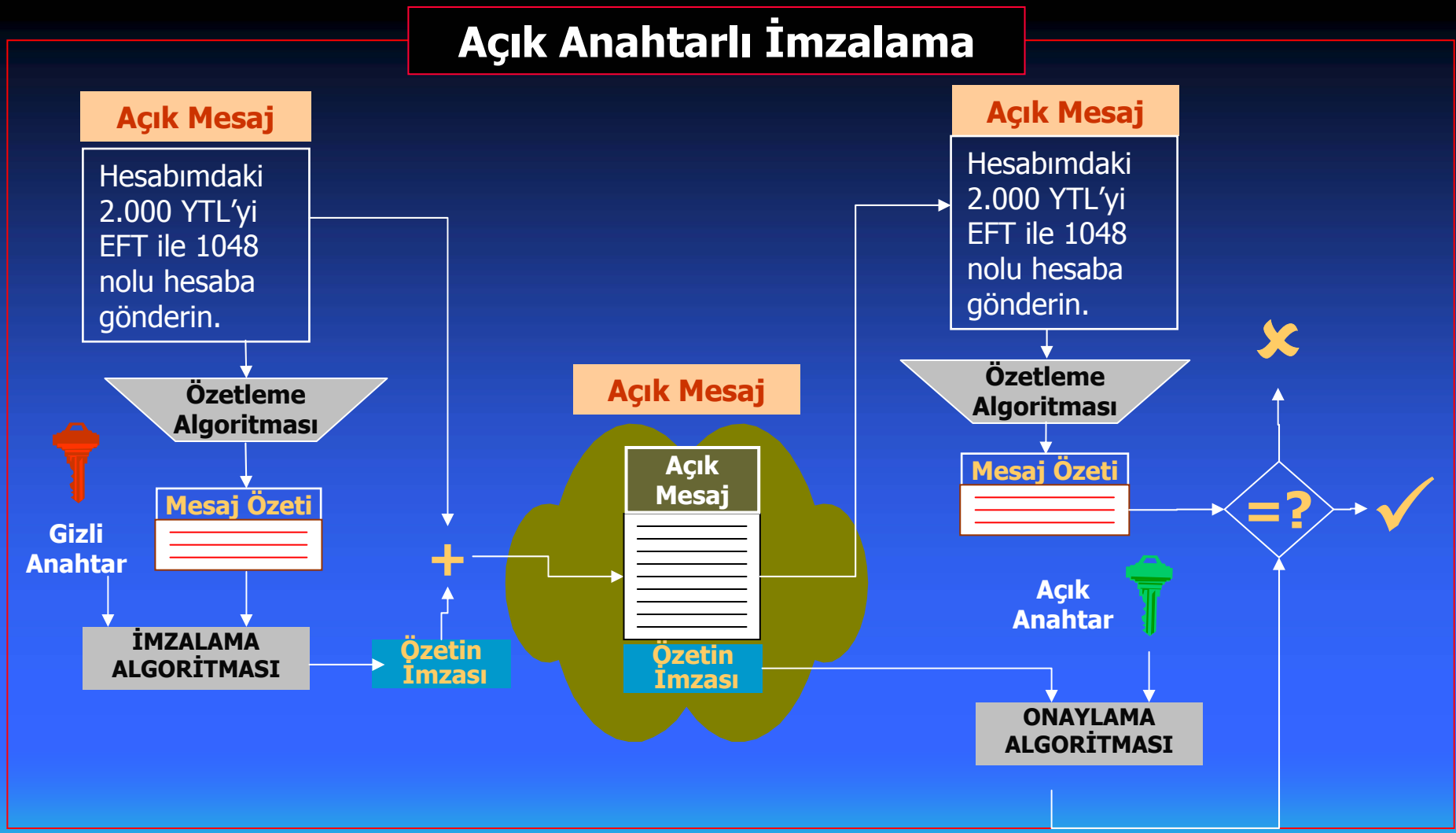
Çözüm: Özetleme fonksiyonu kullanılarak bir "Mesaj Özeti" çıkarılır

- **Özetleme Fonksiyonu**
  - Sabit çıkış uzunluğu (mesajdan çok kısa)
  - Mesajdaki küçük değişiklikler bile özette büyük değişikliklere yol açabilir.
  - Kriptografik tek yönlü fonksiyon
    - Bir mesajın özetini elde etmek kolay
    - Bir özetten asıl mesajı çıkarmak çok zor

Mesaj Özeti


1
Today, ABC Inc. will be announcing the resignation of their CFO. Stock prices are expected...
Original Message
2
Hash Function
3
12a4
3CD68
hh7yt
m onDq5
1 88k Lun
Message Digest

Sayısal İmzada Mesaj Özeti Kullanımı



Sayısal İmza ve Özetleme Algoritmaları

- Sayısal İmza
  - RSA
  - DSA
  - ECDSA
- Özetleme
  - SHA-1 (160 bit)
  - MD5 (128 bit)

AAA Neden Gereklidir?

- Sertifikayı kim verir?
- Özel anahtar nerede saklanır?
- Karşı tarafın özel anahtarının güvende olduğundan nasıl emin olabilirim?
- Sertifikalar nerden bulunup alınır?

Açık anahtar altyapısı (Public Key Infrastructure PKI) gibi sayısal sertifika ve sayısal imza bazlı bir güvenlik sistemi ile yukardaki soruların çözümleri için gerekli temel oluşturulur.

AAA Neden gereklidir?

- Asimetrik kriptografi sistemlerini gerçeklemek için
- Açık ve özel anahtar yönetmek için
  - Kimlik doğrulama
  - İnkar edememezlik
  - Mesaj bütünlüğü
  - Gizlilik

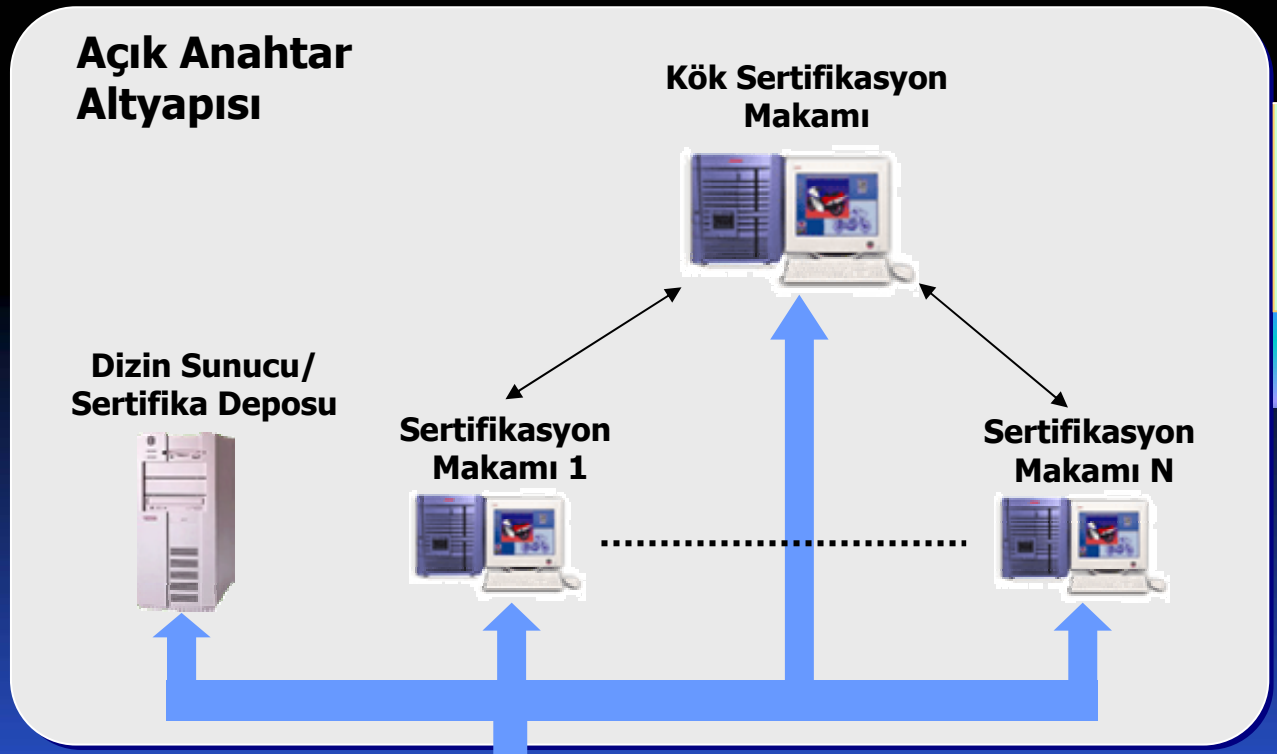
Takdim Planı

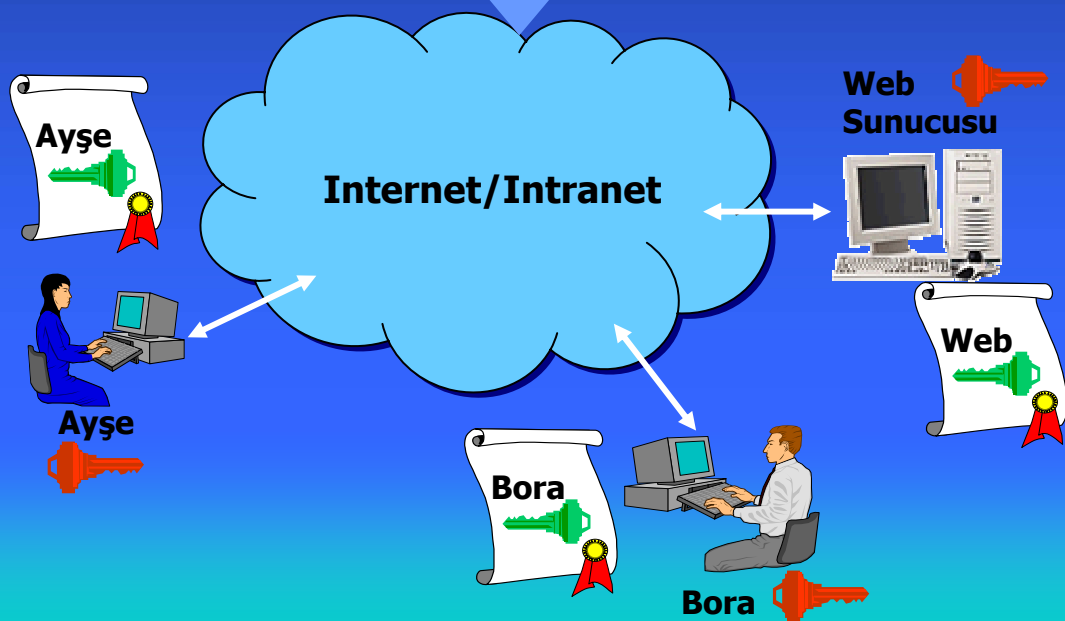
- Giriş
- Temel Kavramlar
- Sayısal (Elektronik) İmza
- Açık Anahtar Altyapısı ile Sayısal İmza Çözümü
- Açık Anahtar Altyapısı Bileşenleri
- Açık Anahtar Altyapısı Mimarileri
- Sonuç

Açık Anahtar Altyapısı ile Sayısal İmza Çözümü

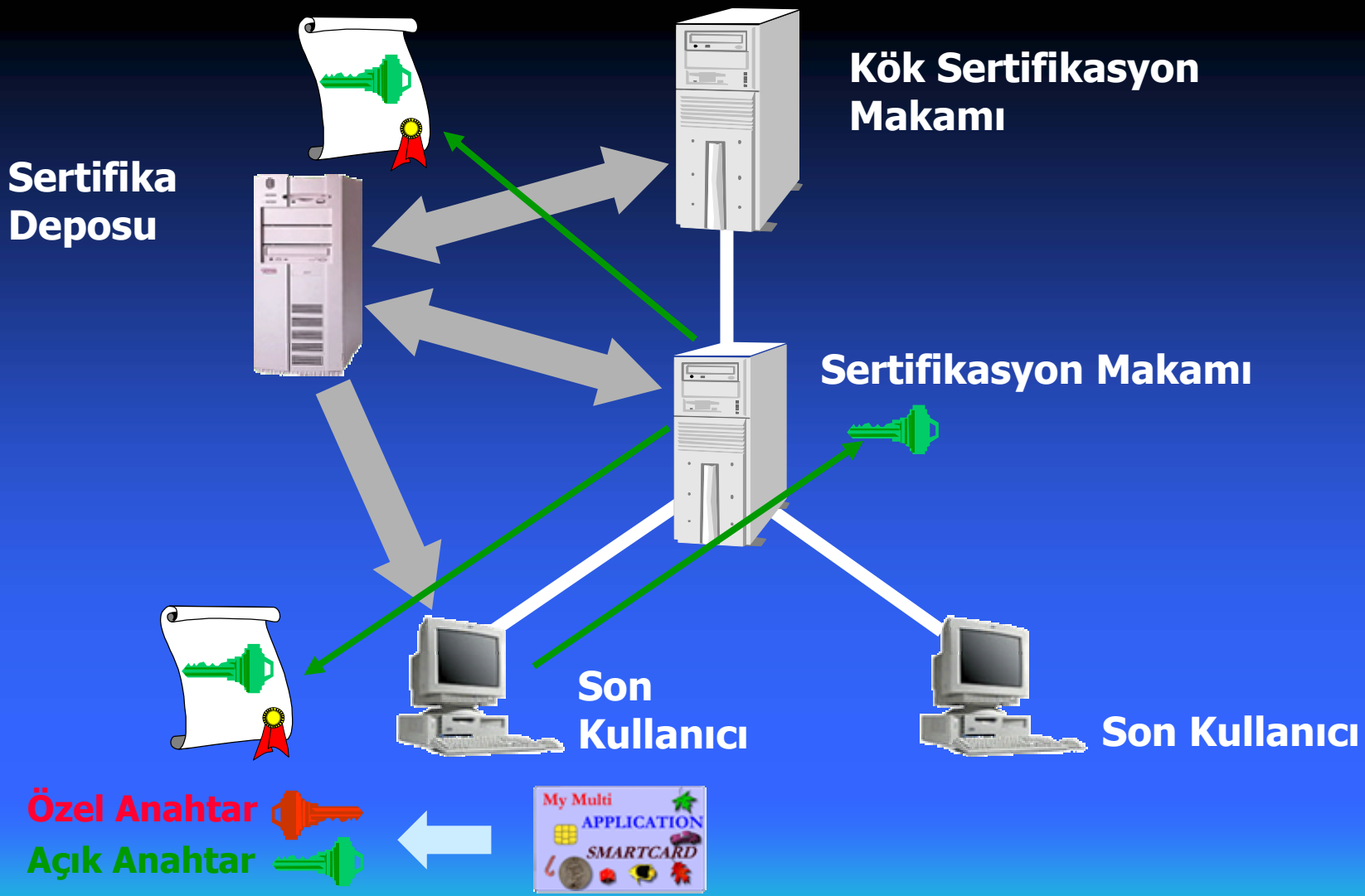
- Açık Anahtar Altyapısı Bileşenleri
- Açık Anahtar Altyapısı ile Sayısal İmza Nasıl Çalışır ?

Açık Anahtar Altyapısı

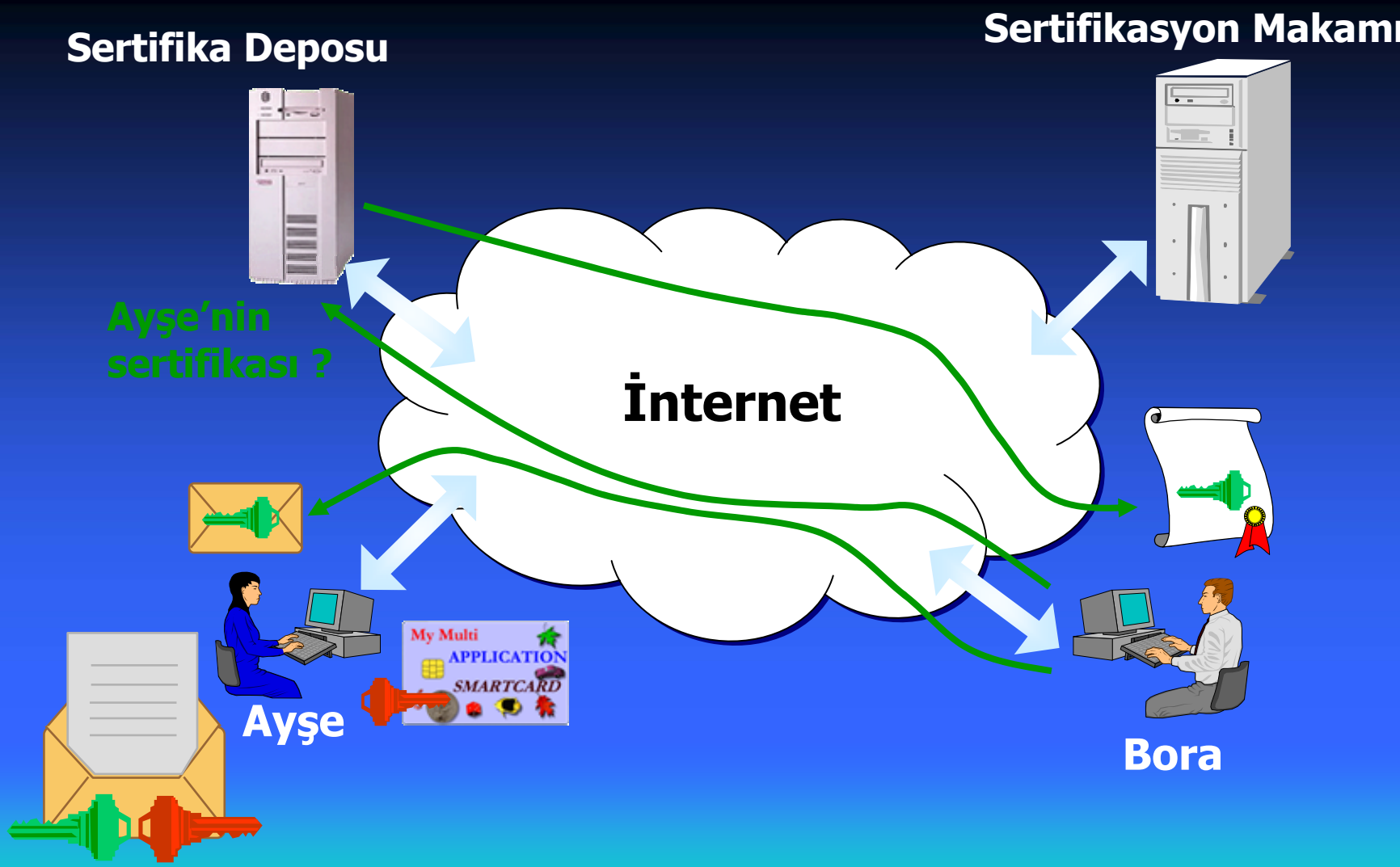




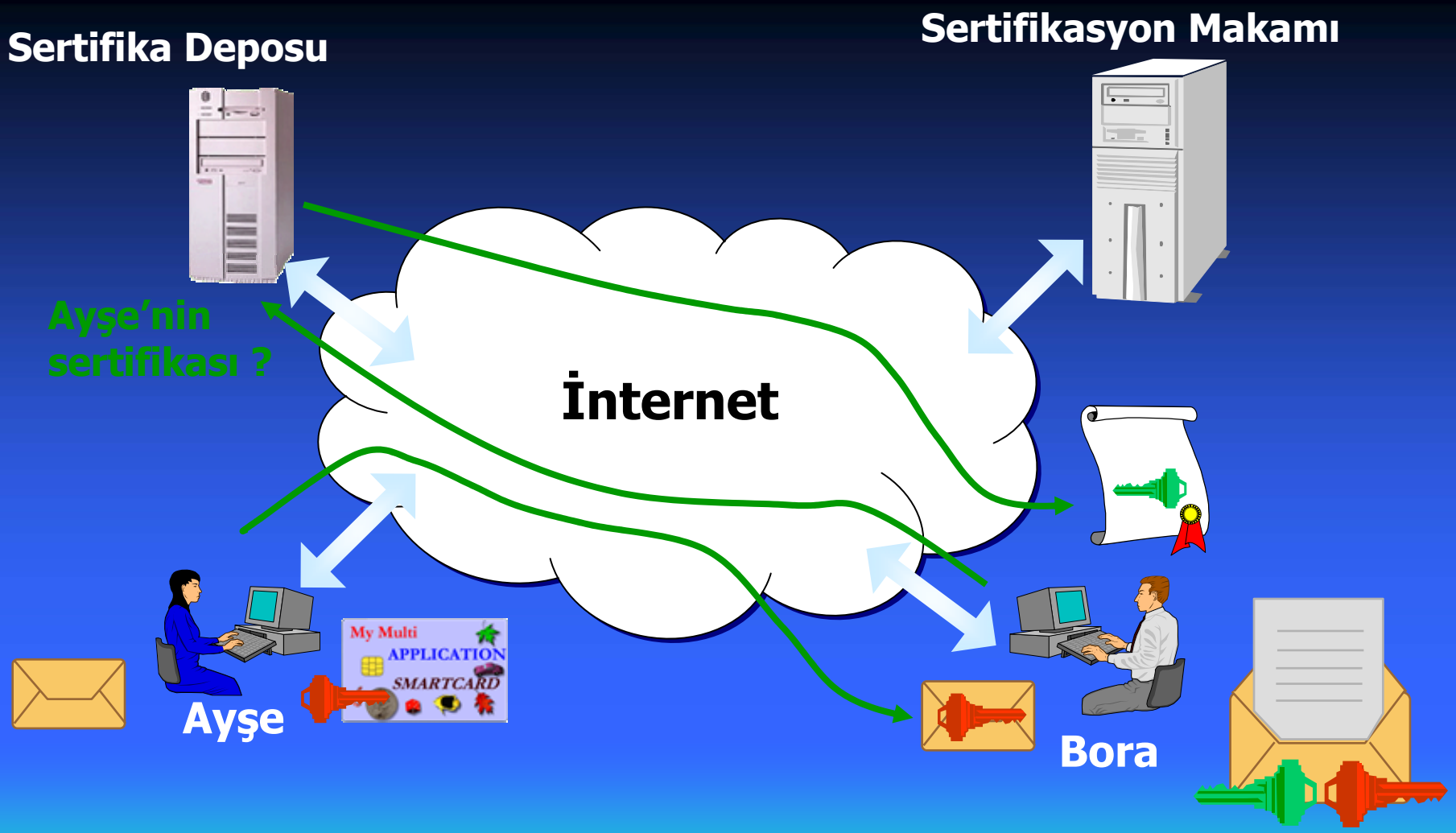
AAA ile Sayısal İmza Nasıl Çalışır ?



AAA ile Şifreli Haberleşme



AAA ile Sayısal İmzalı Haberleşme



Takdim Planı

- Giriş
- Temel Kavramlar
- Sayısal (Elektronik) İmza
- Açık Anahtar Altyapısı ile Sayısal İmza Çözümü
- Açık Anahtar Altyapısı Bileşenleri
- Açık Anahtar Altyapısı Mimarileri
- Sonuç

Açık Anahtar Altyapısı Bileşenleri

- Kök Sertifikasyon Makamı
- Sertifikasyon Makamı
- Kayıt Makamı
- Sertifika Deposu
- Arşiv Modülü
- Sertifika Kullanıcıları
- Kriptografik Anahtar Çiftleri
- Sayısal Sertifikalar
- Sertifika İptal Listesi (SİL)
- Sertifikasyon Prensipleri
- Sertifikasyon Yolu
- Akıllı Kart / Token Cihazları
- AAA Yönetim Protokolleri

Kök Sertifikasyon Makamı

Hiyerarşik olarak en üstte yer alan ve altyapıdaki tüm bileşenlerin elektronik imzasına güvendiği makamdır. Sadece sertifikasyon makamları için sertifika üretir. Son kullanıcılar için sertifika üretmez

Sertifikasyon Makamı

- Donanım, yazılım ve sistemi işleten kişiler sertifika makamını oluşturur.
- Ayırdedici özellikleri; adı ve anahtar çiftidir.
- Görevleri
  - Sertifika yayınlamak
  - Sertifika durum bilgilerini güncel tutmak ve sertifika iptal listeleri (SİL) hazırlamak
  - Güncel sertifikaları ve SİL'leri isteyen kişilere sunmak
  - Süresi dolan ya da iptal edilen sertifikaların arşivini tutmak

Kayıt Makamı

- Sertifika makamı için sertifika başvurularını alır ve sertifika içine yerleştirilecek bilgilerin doğruluğunu kontrol eder.
- Topladığı bilgilerden bir sertifika isteği oluşturur.
- Kayıt makamı topladığı bilgileri SM'ye kendi sayısal imzasıyla imzalayarak iletir. Böylece SM sertifika isteğinin güvendiği bir kaynaktan gelip gelmediğini anlayabilir.
- Kendi özel anahtarını çok iyi korumalıdır.
- Birden çok SM için bu hizmeti verebilir.

Sertifika Deposu

- Sertifikaların ve sertifika iptal listelerinin dağıtımını yapar.
- Birden çok SM'nin sertifika ve SİL'lerini depolayabilir.
- Kendi başına çalışan ve belli bir erişim protokolünü (ör: LDAP) kullanan bir bilgisayar sistemidir.
- Güvenilir değildir; içindeki sertifikalara ve SİL'lere güvenilmesinin sebebi SM tarafından sayısal imza ile korunmuş olmalarıdır.
- Barındırdığı sertifika ve SİL'leri sadece yetkili kişiler güncellemelidir. Aksi bir durumda saldırganlar depo içindeki bilgileri kullanılmaz hale getirip AAA'nın çalışmasını engelleyebilir.

Arşiv Modülü

- Arşivleme bileşeni uzun dönemli veri saklama görevini SM adına yapan modüldür.
- Arşivleme modülü bilginin kendisine ulaştığında doğru olduğunu ve geçen süre içinde değişmediğini garanti altına alır.
- Arşivlenecek bilgiler (sertifika ve SİL) SM tarafından arşiv modülüne iletilir.
- İlerde doğabilecek bir anlaşmazlıkta (örneğin eski bir dokümandaki sayısal imzanın kontrolünde) geçmiş tarihli sertifikanın arşiv modülü tarafından isteyen taraflara verilebilmesi gereklidir.

Sertifika kullanıcıları

- SM'ye veya KM'ye sertifika talebinde bulunurlar.
- SM, KM, bilgi sistem birimi (router, firewall, web server vb) ya da kişiler olabilir.
- Aldıkları sertifika ile bir özel ve bir açık anahtar sahibi olurlar ve
  - Sayısal imza
  - Simetrik anahtar değiş tokuşu (güvenli haberleşme)
  - Kimlik doğrulama

  gibi işlemleri yaparlar.

Sertifika Kullanıcıları

- SM'yi güvenilen taraf olarak kabul ederler.
- Sertifika deposundan iletişim kurmak istedikleri kişinin sertifikasını ve SM'nin yayınladığı SİL'leri alırlar.
- Sertifikaları kullanarak karşı tarafın sayısal imzasını ve kimliğini doğrulayabilirler.
- Sertifikasyon yolunu oluşturur ve doğrularlar.
- Sertifika deposu ile anlık haberleşirler.

Kriptografik Anahtar Çiftleri

AAA sisteminde her kullanıcı için açık ve özel anahtar çiftleri üretilir. İmzalama, şifreleme, imza onaylama ve şifre çözme işlemlerinde bu anahtar çiftleri kullanılır. Kullanıcının açık anahtarı tüm kullanıcılara dağıtılırken, özel anahtar ise sadece kullanıcı tarafından bilinir

Anahtar Yaşam Döngüsü

Sayısal İmza Sertifikaları

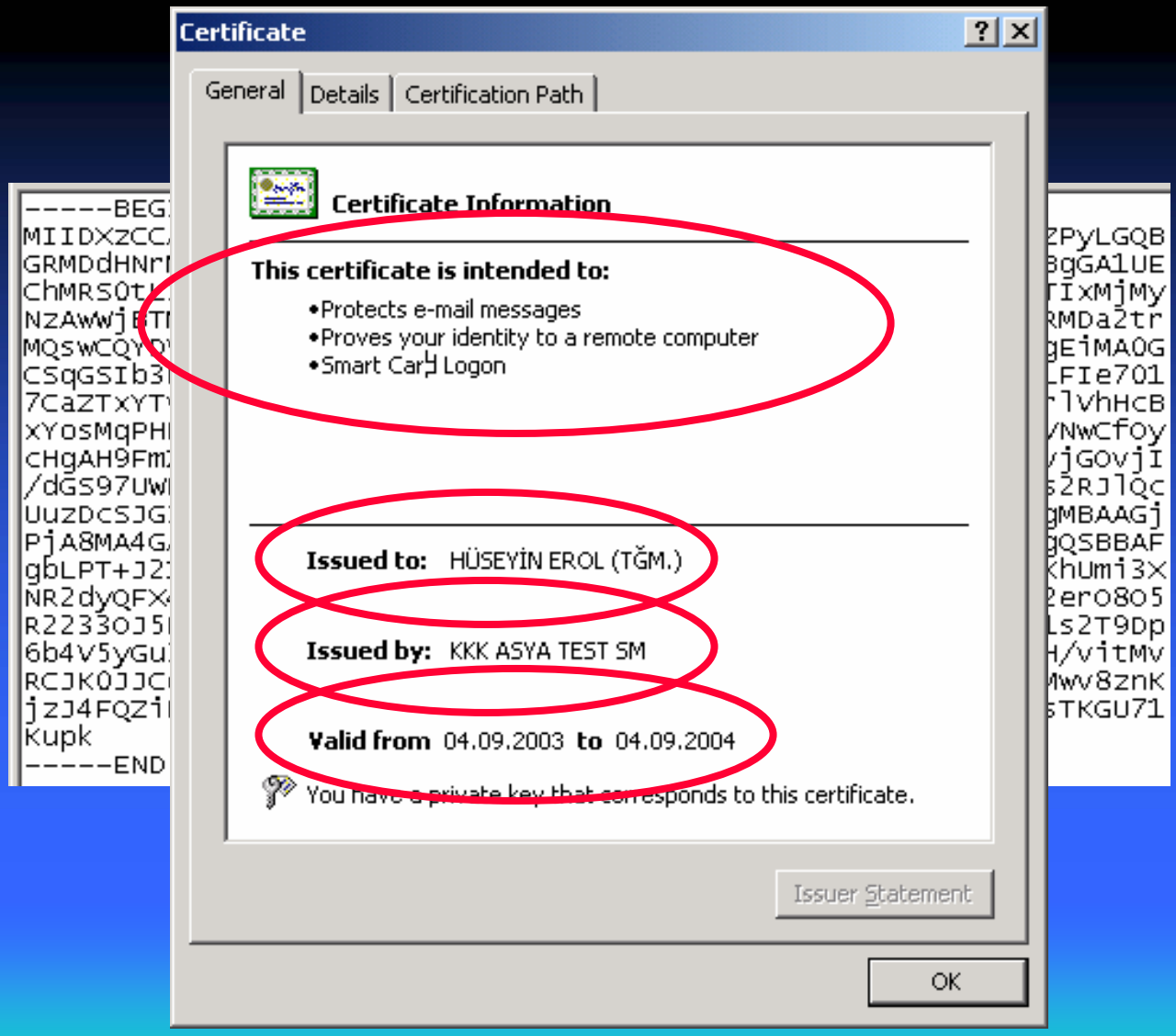
- Sayısaldır, bilgisayarda hazırlanır. (X.509)
- Sahibinin adını ve açık anahtarını içerir.
- Sahibinin çalıştığı şirketin/kurumun adını içerir.
- Genelde sahibinin e-posta adresini içerir.
- Kullanıma giriş tarihini ve son kullanım tarihini içerir.
- Yayınlayan güvenilir kurumun adını içerir.
- Yayınlayan kuruluş tarafından verilmiş tekil bir seri numarasına sahiptir.
- İçeriğin bütünlüğü yayınlayan kuruluşun sayısal imzasıyla koruma altına alınmıştır.
- Sertifikanın bütünlüğünün bozulması engellenemez ama böyle bir durum sayısal imzanın kontrol edilmesiyle hemen anlaşılır.

Örnek Sertifika

Seri No	2368
Sertifika Sahibi	Hüseyin EROL
Kurum	Gazi Üniversitesi
Yayınlayan	Tübitak
E-posta Adresi	Herol @ gazi.edu.tr
Yayın Tarihi	01.12.2004
Son Kullanım	01.12.2005
Açık Anahtar	2489349e894859f45489450dab4545 4ca0908d8809

Tübitak Sayısal İmzası	Ae89349c989893e8989548d0823048 b08023f9e903hsasde345l62m234

Açık Anahtar Sertifikaları (Örnek Sertifika)



Sertifikaların bütünlüğü nasıl korunuyor?

Sertifika alanları:

- **Sertifika sahibinin TKA**
- **Sertifika yayınlayıcısı TKA**
- **İmzalama algoritması**
- **Açık anahtar algoritması**
- **Açık anahtarın kendisi**
- **Sertifika geçerlilik tarihi**
- **Sertifika seri numarası**
- **Versiyon**
- **Eklentiler**

Sertifika Makamının İmzası

- Sertifika byte'lardan (sekizli) oluşur.
- Sertifikasyon makamı sarı ile gösterilen alanı kendi özel anahtarı ile imzalayıp önceki byte'ların arkasına ekler.

Sertifika İptal Listeleri (SİL - CRL)

- Sertifika içeriğinin güncel olup olmadığı sorusuna cevap vermek
  - Sertifika sahibinin erişim bilgileri değişmiş olabilir
  - Sertifika sahibi özel anahtarını kaybettiği için yeni bir açık anahtar kullanmaya başlamış olabilir.
  - Sertifika sahibi sertifikasını dağıttıktan sonra geri toplayamaz; değişiklikleri duyurması çok zordur.

Sertifika İptal Listesi

- Sayısaldır.
- Artık güvenilemeyecek olan ve kullanım süresi dolmamış sertifikaların seri numaralarını içerir.
- Yayın tarihini ve son kullanım tarihini içerir.
- Yayınlayan kuruluşun adını ve sayısal imzasını içerir.
- Sık aralıklarla Internette yayınlanır.

Örnek SİL Sertifikası

Yayınlayan	**Tübitak**
Yayın Tarihi	**01.12.2004**
Son Kullanım	**20.12.2004**

İptal Olan Sertifikaların Listesi
55, 678, 2164, 3403, 4034, 5677 ....

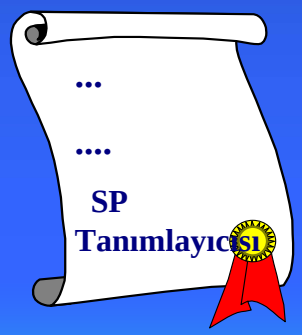
Tübitak Sayısal İmzası	6656e345200cde989228d08 23aec8b08023f9

Online Certificate Status Protocol(OCSP)

- SİL'lerin bir periyot boyunca geçerli olması, bu periyot boyunca iptal edilen sertifikalardan kullanıcıların bir sonraki periyotta haberinin olmasına yol açamaktadır.
- Çözüm: Online Certificate Status Protocol
  - Her SM'ye ait bir veya birden fazla sertifikalandırdığı OCSP sunucusu olabilir. OCSP sunucu o SM'nin yayınladığı sertifikaların iptal edilip edilmediği bilgisine ulaşır.
- RFC 2560 Online Certificate Status Protocol

Sertifikasyon Prensibi (SP)

- Sertifikasyon Prensibi, sertifika dağıtmak ve sertifika bilgilerini tutmak için güvenlik politikalarının yazıldığı genel bir dokümandır.
- **Neler**in yapılması gerektiğini belirler
- Zamanla değişecek, uygulamadaki detayları içermez.
- Bir sertifika içerisinde tekil bir SP referansı vardır. (Sertifika Prensibi OID)



Sertifikasyon Prensipleri

Seri No	2368
Sertifika Sahibi	Hüseyin EROL
Kurum	Gazi Üniversitesi
Yayınlayan	Tübitak
E-posta Adresi	Herol @ gazi.edu.tr
Yayın Tarihi	01.12.2004
Son Kullanım	01.12.2005
Prensip	E-posta imzalama, dosya imzalama
Açık Anahtar	2489349e894859f45489450dab4545 4ca0908d8809
Tübitak Sayısal İmzası	Ae89349c989893e8989548d0823048 b08023f9e903hsasde345l62m234

Sertifika Uygulama Kuralı (SUK)

- SM'nin bir SP'yi nasıl gerçekleyeceğini detaylı anlatan dokümandır
- Bir SM tarafından, sertifika yayınlamakta kullanılan ayrıntılı işlemleri anlatan bir dizi ifadedir
- Tek SUK, birden çok SP'yi destekleyebilir
- Farklı SUK'ları olan SM'ler aynı SP'yi kullanarak birlikte çalışabilir

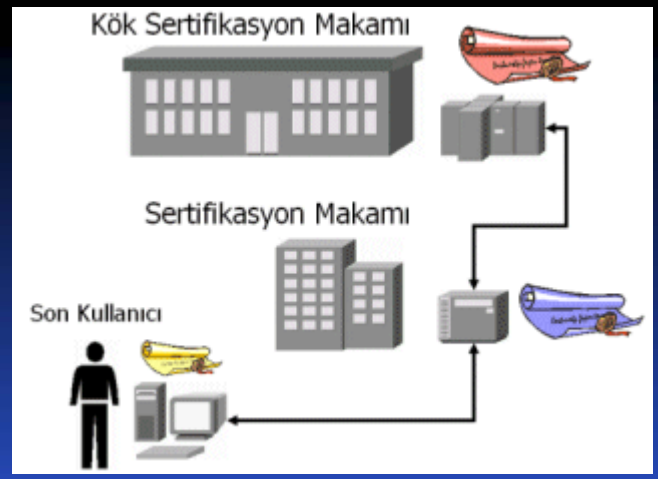
SUK - SP

- SP, bir sertifikanın hangi emniyet düzeyini sağlayacağını belirtir
- SUK, SP'de belirtilen emniyet düzeyinin **nasıl** gerçekleneceğini ayrıntılı olarak ortaya koyar
- Bir SUK, belli bir SM için hazırlanır.
- Bir SP, SUK'dan daha globaldir ve başka SM'lere de uygulanabilir.

SUK-SP (Örnek)

- SP
  - Kullanıcılar, özel anahtarlarının yetkisiz şahısların eline geçtiğini farkettiklerinde, zaman kaybetmeden İşletme Makamı'na haber vereceklerdir
- SUK
  - Tüm kullanıcılar (son kullanıcı SM operatörleri dahil), özel anahtarlarının yetkisizce açığa çıkması durumlarında, bu durumu bildirmeleri gerektiği konusunda bilgilendirilmelidir.
  - Özel anahtarların yetkisizce açığa çıkarılması durumu tespit edilirse, kullanıcılar 1 iş günü içerisinde bağlı oldukları SM ile bağlantıya geçeceklerdir. SM ile bağlantıya geçme yöntemi, SUK içerisinde belirtilen yöntemlerden biri şeklinde olabilir.
  - Kullanıcılar, kullanımda olmadığı zaman özel anahtarlarını, üzerlerinde taşımalılar veya kilitle korunan bir yerde tutmalıdırlar

Sertifikasyon Yolu



- Ölçeklenebilir bir sistem
- Sertifika yöntemi hiç tanımadığımız kişilere güvenilir bir kurum aracılığıyla güvenmemizi sağlıyor
- Haberleştiğimiz bir kişi herhangi bir yayıncı kuruluştan sertifika almış olabilir
- Kişi/kurum e-posta koruması, sözleşme onaylama, web güvenliği sertifikalarını ayrı ayrı yayıncılardan alabilir

Sertifikasyon Yolu

- Güvenilen tüm sertifika yayıncılarını bir listede tutabilir
- Bir sertifika yayıncısı diğer yayıncıların güvenilirliğini gösteren sertifikalar yayınlayarak bir sertifikasyon zinciri ya da hiyerarşisi yaratabilir.
- İki sertifika yayıncısı birbirlerine güvendiklerini gösteren sertifikalar yayınlayarak çapraz sertifikasyon yapabilirler.

Akıllı Kart / Token Cihazları

- Akıllı kartlar kullanıcılara ait özel anahtarların muhafaza edilmesi için en güvenli ortamı sunar.
- Akıllı kartlar, programlanabilir alanları olan, dayanıklı, taşınabilir bilgisayarlardır.
- Bir kredi kartı ile aynı büyüklükte ve şekildedir.
- Veri güvenliği, kimlik gizliliği ve mobil kullanıcı ihtiyaçlarına sahip sistemlerde faydalıdır.

Akıllı Kartlar ve Kullanımları

- Akıllı kartların private ve public alanları vardır.
- Private alanında anahtar üretimi, imzalama, şifre çözme gibi işlemler yapılır, bu alana erişim yasaklanmıştır.
- Public alana genel bilgiler yazılır. Akıllı kart programı yardımıyla buradaki bilgiler görülebilir.
- Bir PKI akıllı kartında minimum olması gerekenler :
  - İmzalama özel anahtarı
  - Şifreleme özel anahtarı
  - O an geçerli olan imzalama sertifikası
  - O an geçerli olan şifreleme sertifikası
  - Daha önce geçerli olan şifreleme özel anahtarları ve karşılığı olan sertifikaları

AAA Yönetim Protokolleri

- SM,
  - sertifika ve SİL'leri doğru bir biçimde yayınlamalı
  - Kendi özel anahtarını korumalı
  - Kendini AAA'nın diğer bileşenleriyle haberleşirken korumalı
- AAA Yönetim protokolleri, bilgi toplamak ve yayınlamak için kullanılır.

Yaygın Olarak Kullanılan Yönetim Protokolleri

- PKCS #10 Sertifika Talep Standardı ve SSL
- PKCS #10 Sertifika Talep Standardı ve PKCS #7
- Sertifika Yönetim Protokolü (CMP)
- Certificate Management Using CMS
- Simple Certificate Enrollment Protocol

PKCS Standartları

- #1: RSA açık anahtar algoritması kullanarak şifreleme ve sayısal imzalama işlemi yapılmasını tanımlar. (var)
- #3: Diffie-Hellman anahtar belirleme protokolünü tanımlar.
- #5: Bir şifre kelimesinden elde edilen gizli anahtarla şifrelemenin nasıl yapılacağını anlatır. (var)
- #7: Sayısal imzalama ve şifrelemede kullanmak üzere kriptografik yöntemleri destekleyen genel bir mesaj formatı tanımlar. (var)
- #8: Değişik açık anahtar algoritmalarında kullanılabilecek bir özel anahtar formatı tanımlar. (var)
- #9: Diğer PKCS standartlarında kullanılabilecek nitelik tiplerini tanımlar. (var)
- #10: Sertifika talep formatını tanımlar. (var)
- #11: Kriptografik cihazlarda (akıllı kart vb.) kullanılabilecek donanım bağımsız bir programlama kütüphanesini tanımlar. (Crpytoki) (var)
- #12: Bir kullanıcının özel anahtarı, sertifikası gibi bilgileri saklamak ve taşımak için bir format tanımlar.(var)
- #13: Eliptik eğri kriptografi kullanarak şifreleme ve sayısal imzalamayı tanımlar.
- #14: Pseudo-random sayı üretimini tanımlar (geliştirme aşamasında)
- #15: PKCS#11'i tamamlayan bir standarttır. Kriptografik cihaz tiplerini çeşitlendirir.

Takdim Planı

- Giriş
- Temel Kavramlar
- Sayısal (Elektronik) İmza
- Açık Anahtar Altyapısı ile Sayısal İmza Çözümü
- Açık Anahtar Altyapısı Bileşenleri
- Açık Anahtar Altyapısı Mimarileri
- Sonuç

Açık Anahtar Altyapısı Mimarileri

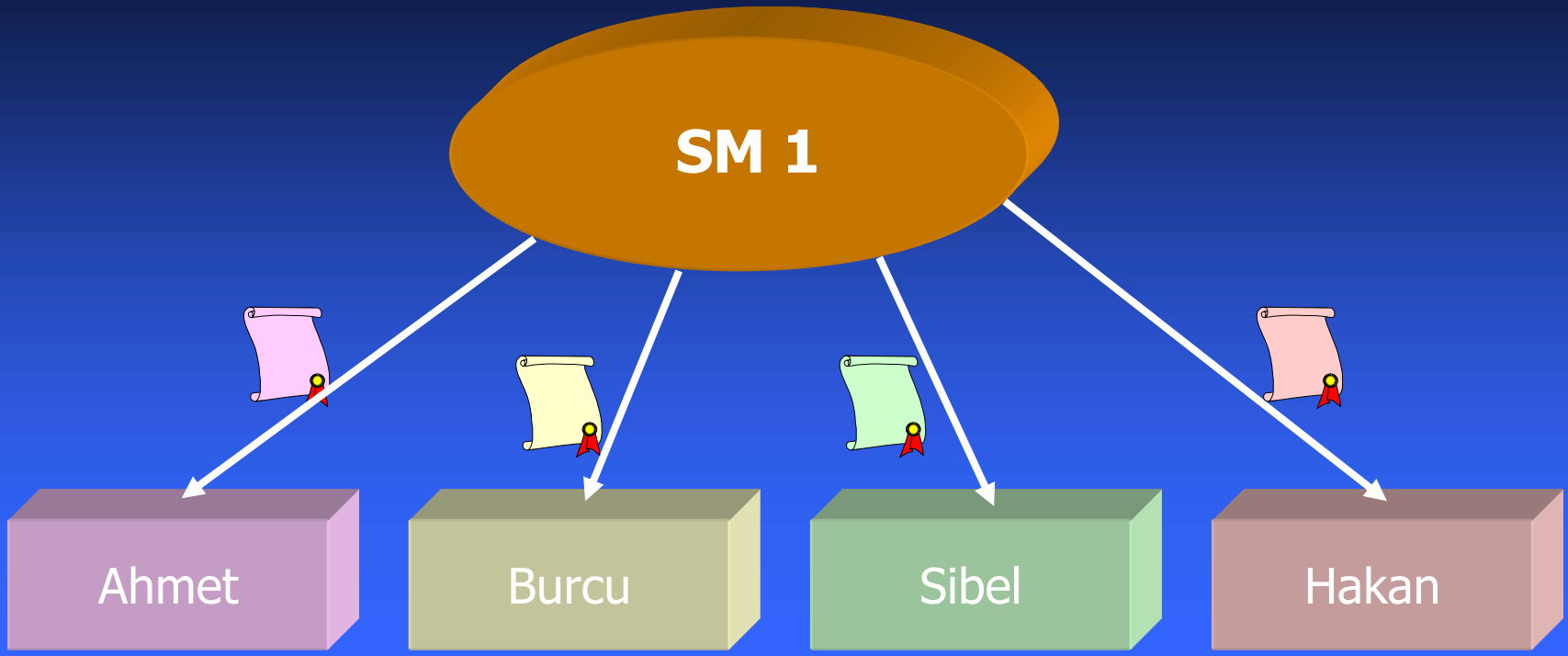
- Basit Mimariler
- Hiyerarşik Mimariler
- Dağıtık Mimariler
- Genişletilmiş SM Listesi
- Çapraz Sertifikasyon
- Sertifikasyon Köprüsü

AAA Mimarisi

- Kaç tane sertifika makamı güvenilir kabul edilecek?
- Sertifika makamları arasında ne tür ilişkiler var?
- Yeni sertifika makamları sisteme ne kadar kolay (ya da zor) ekleniyor?
- Sertifikasyon yolunun oluşturulması ne kadar karışık? Sertifikasyon yolu kurulduktan sonra doğrulama ne kolaylıkta yapılabiliyor?
- Bir sertifika makamı kullanılamaz hale gelirse (güvenilirliğini kaybederse, ulaşılamaz duruma gelirse vb.) sistem bundan nasıl etkileniyor? Bu durumdaki bütün SM'lerin etkisi aynı mı olur?

Basit Mimariler - Tek SM

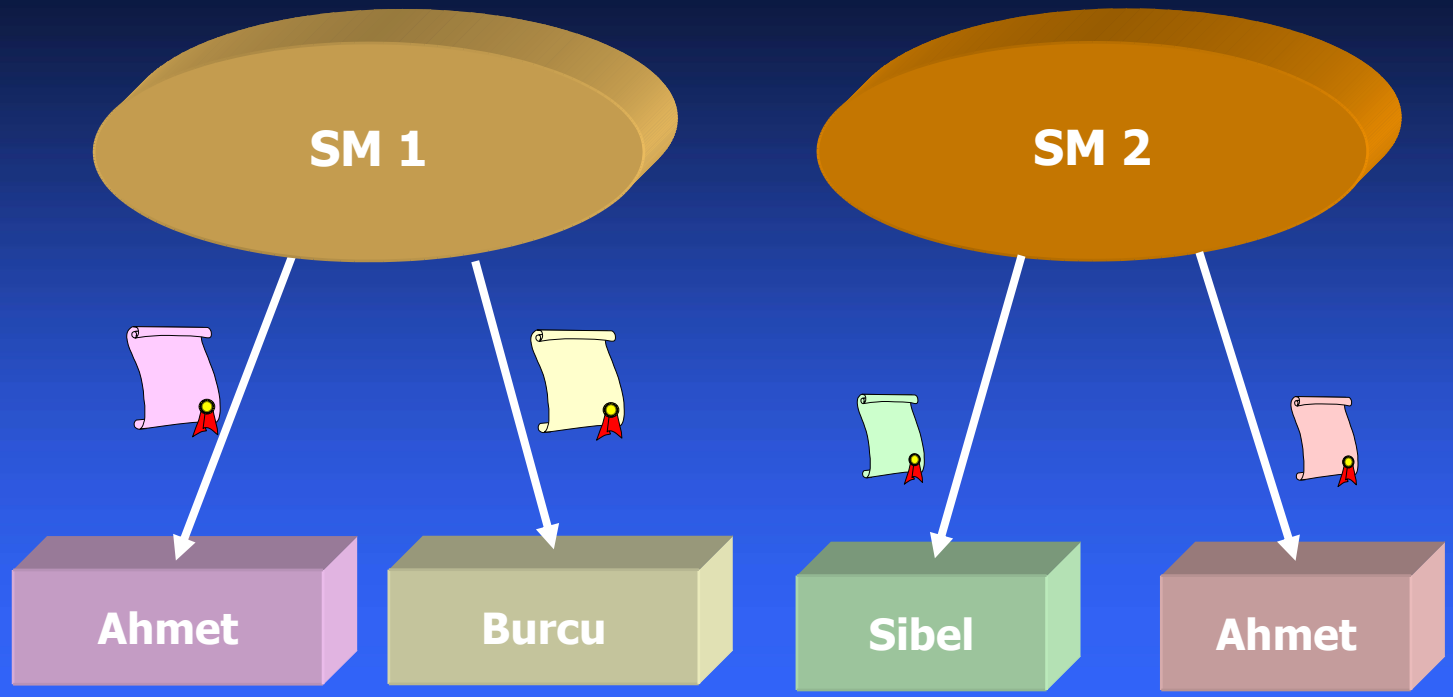
Tek Sertifika Makamı Kullanan Sistem



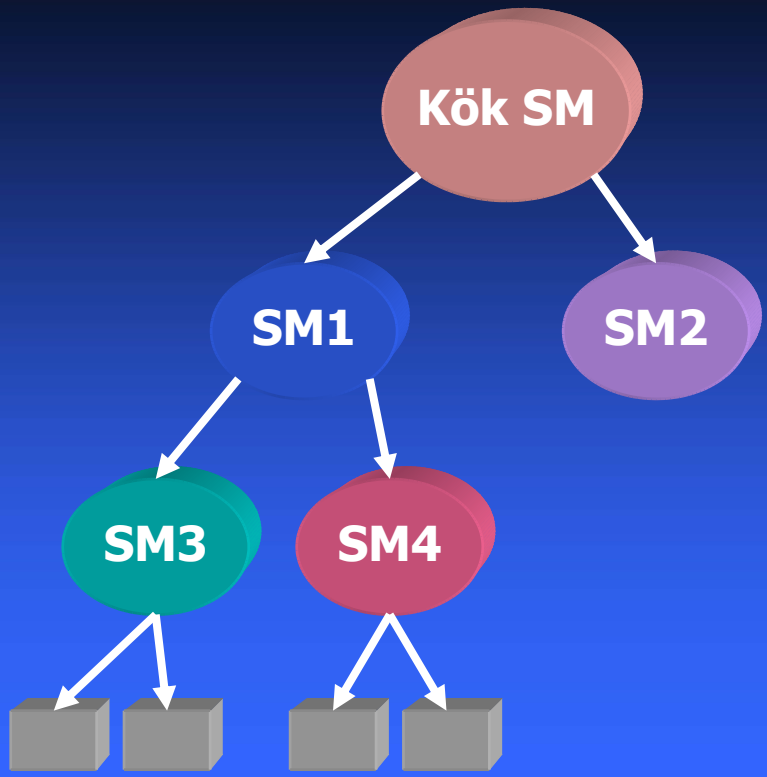
Basit Mimariler – SM Listesi

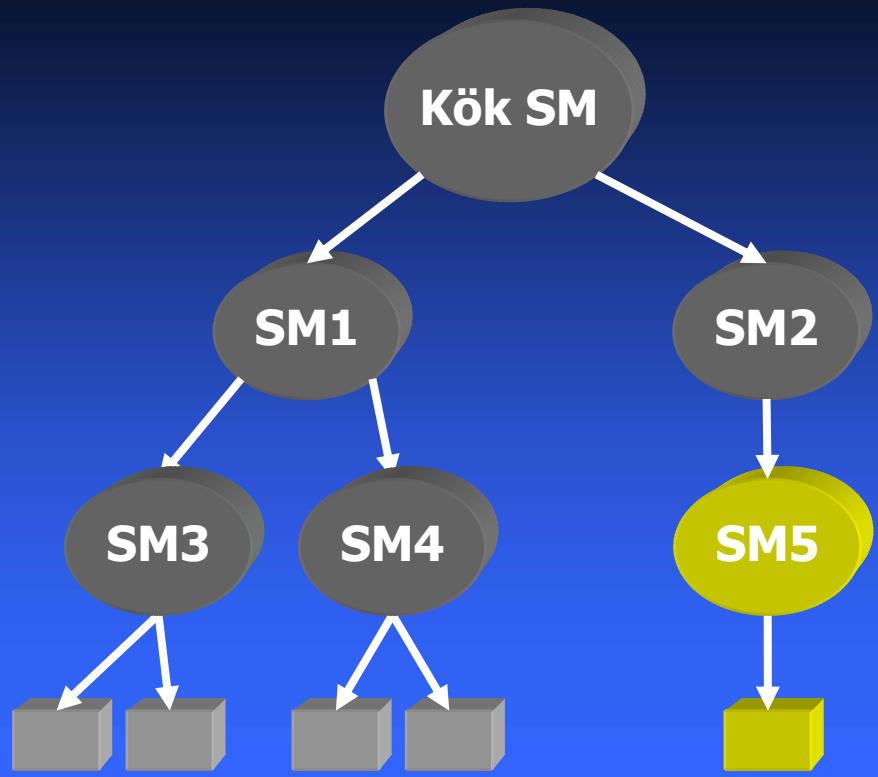
Ahmet'in SM Listesi

SM 1
SM 2



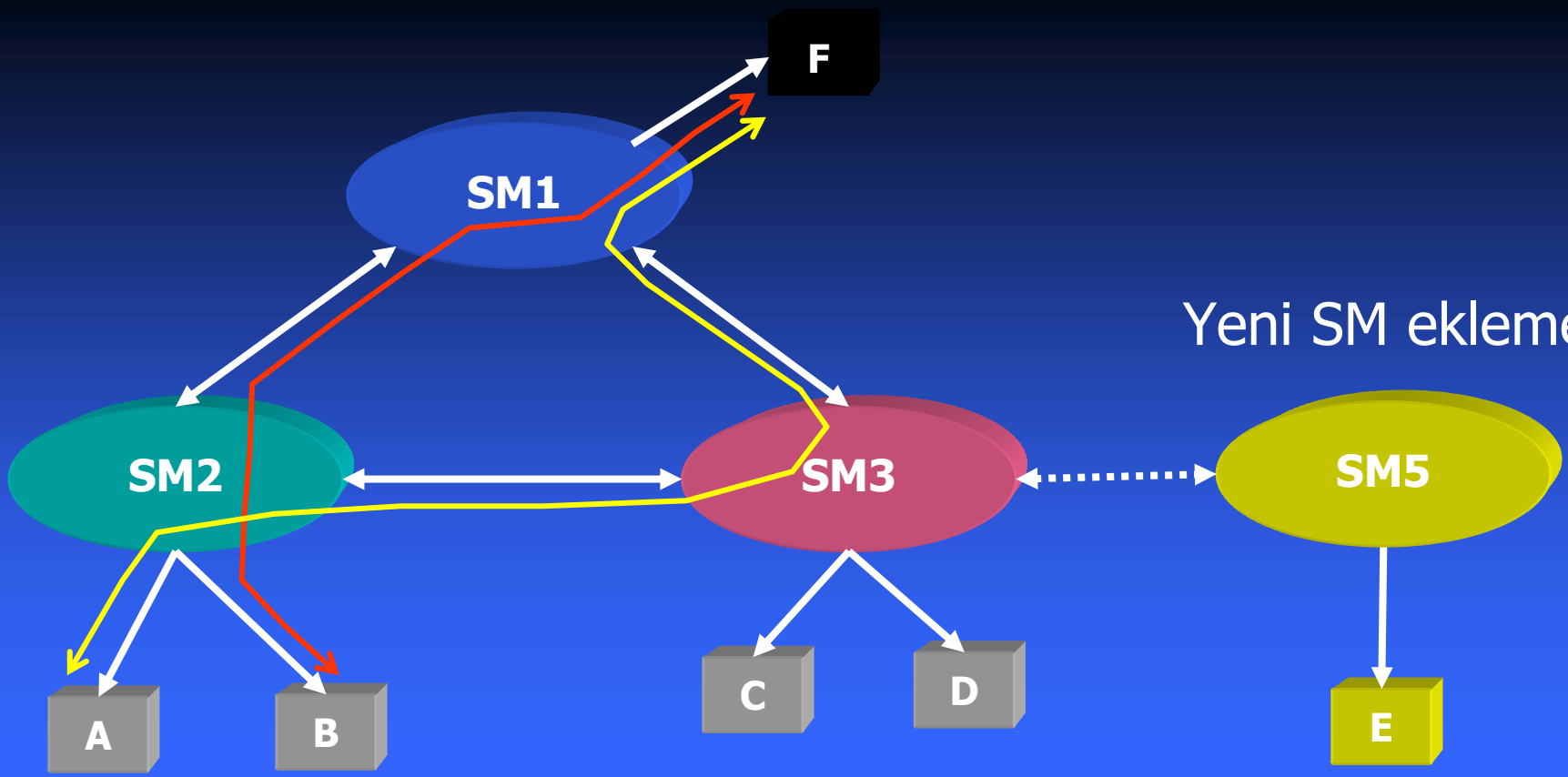
AAA Mimarisi - Hiyerarşik



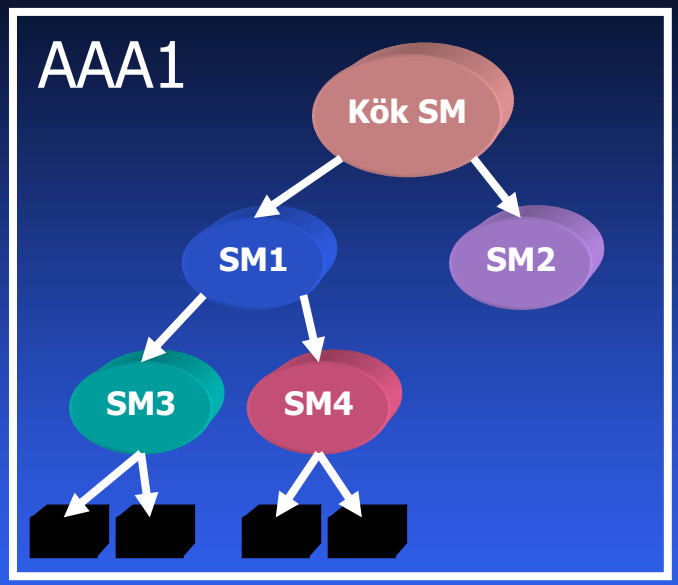


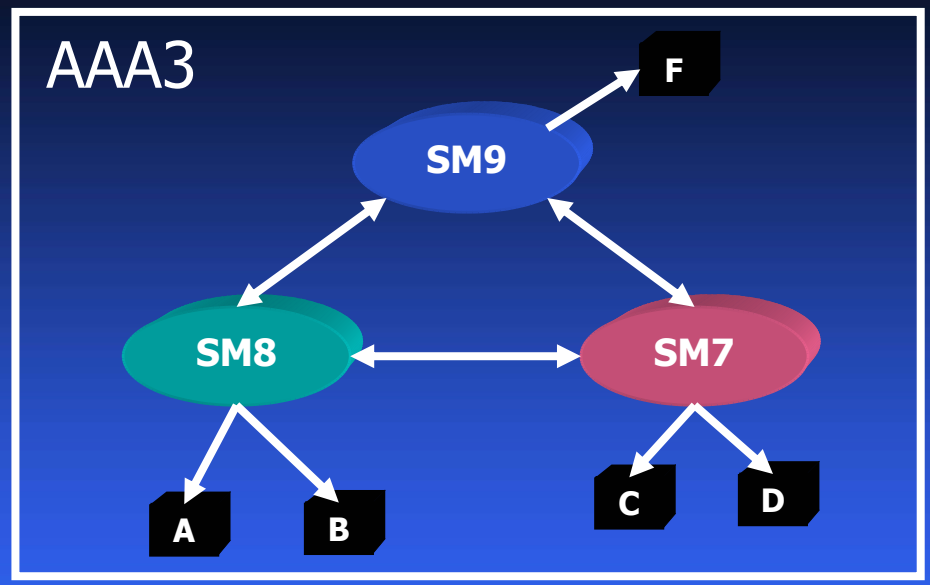
Yeni SM eklemek kolaydır

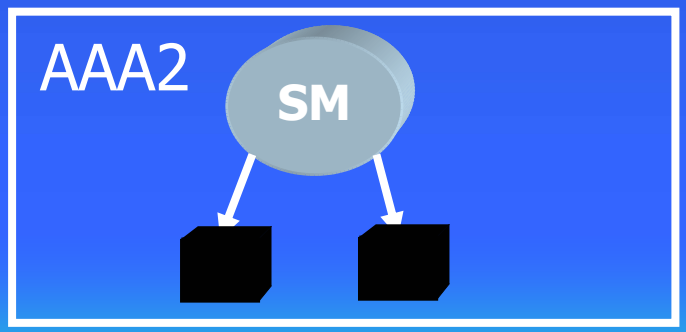
AAA Mimarisi - Dağıtık



AAA Mimarisi Genişletilmiş SM Listesi



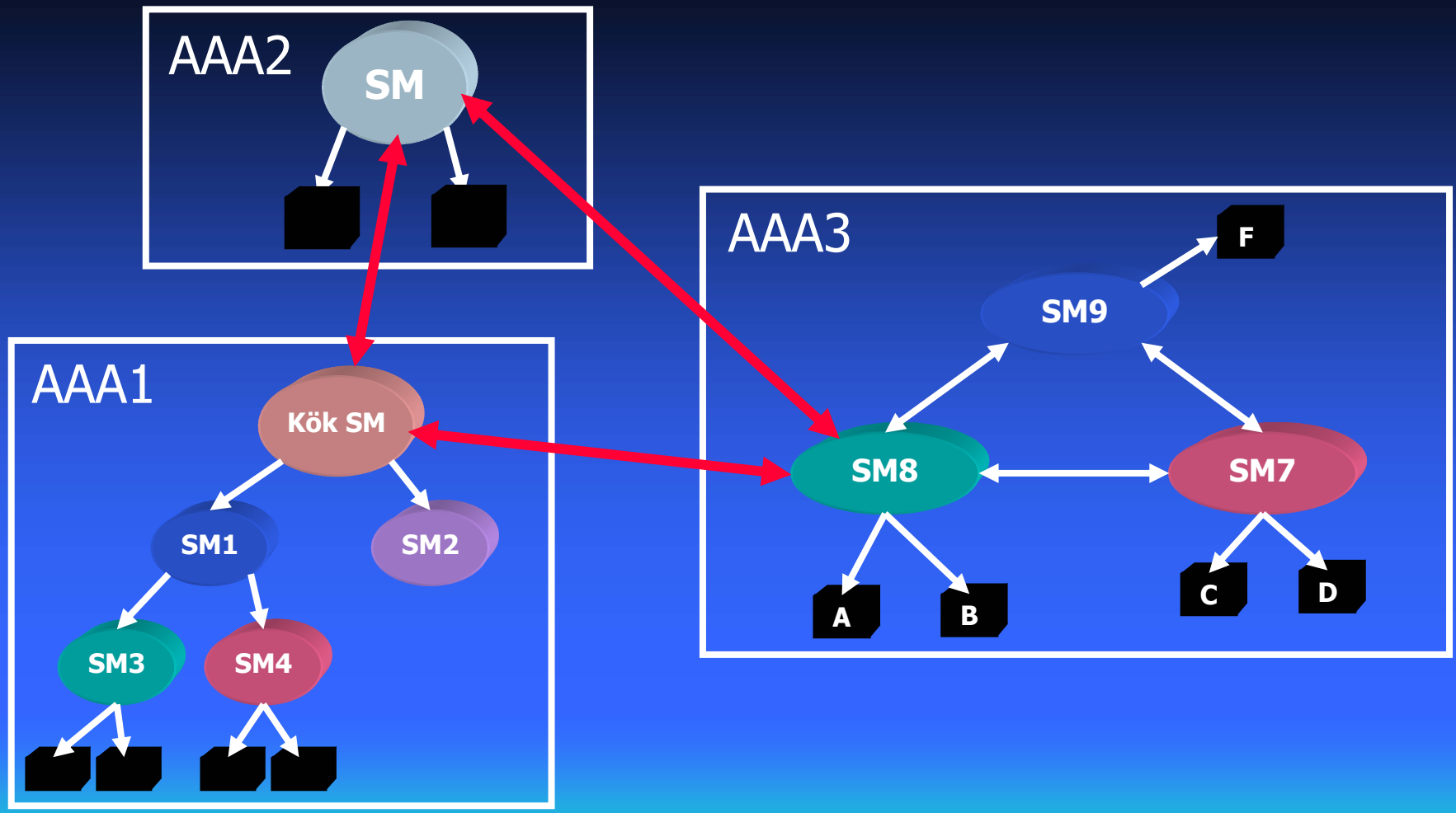




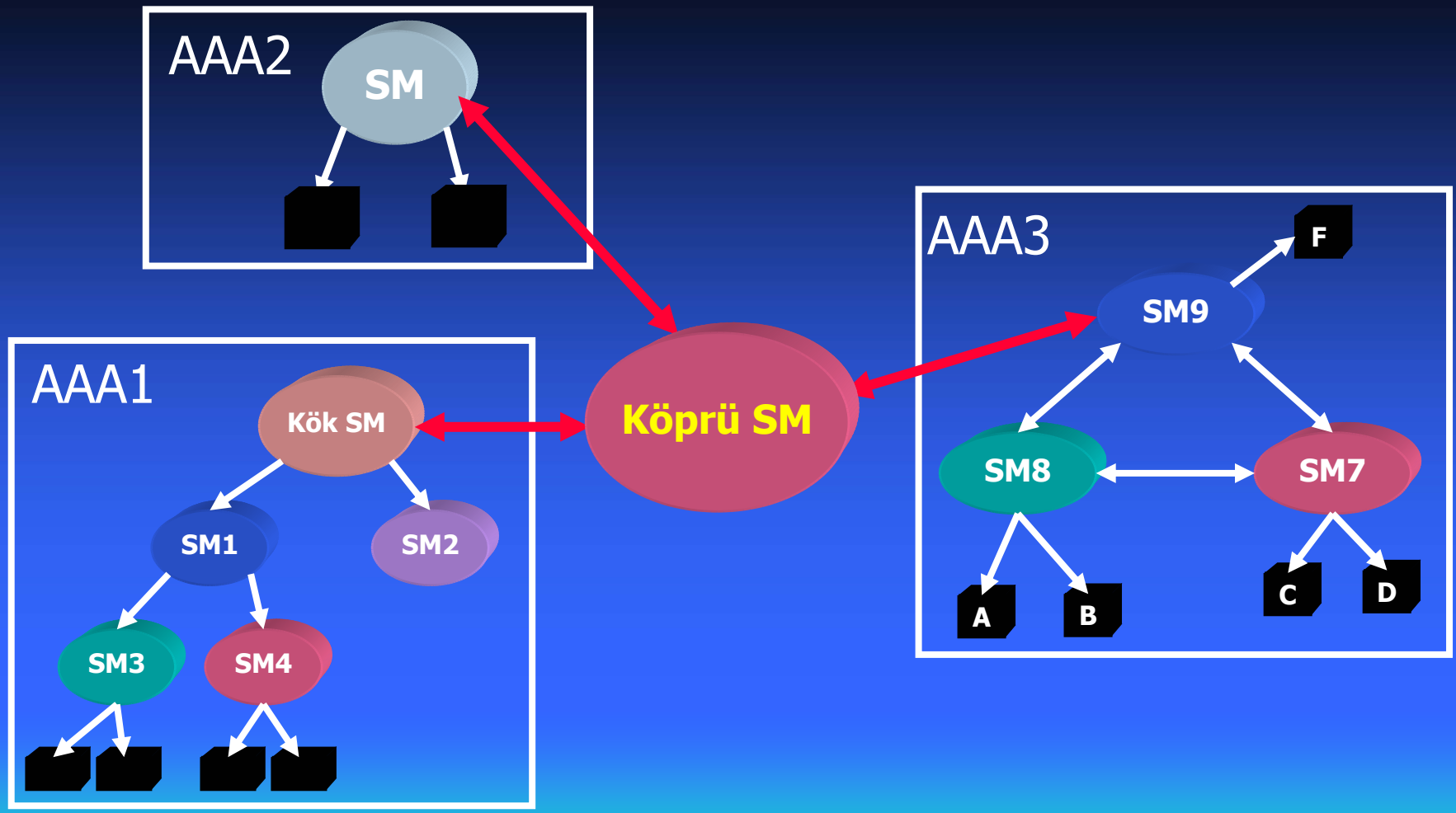
Ahmet'in SM Listesi

AAA1 Kök SM
AAA2 SM
AAA3 SM8

AAA Mimarisi Çapraz Sertifikasyon



AAA Mimarisi Sertifikasyon Köprüsü



Takdim Planı

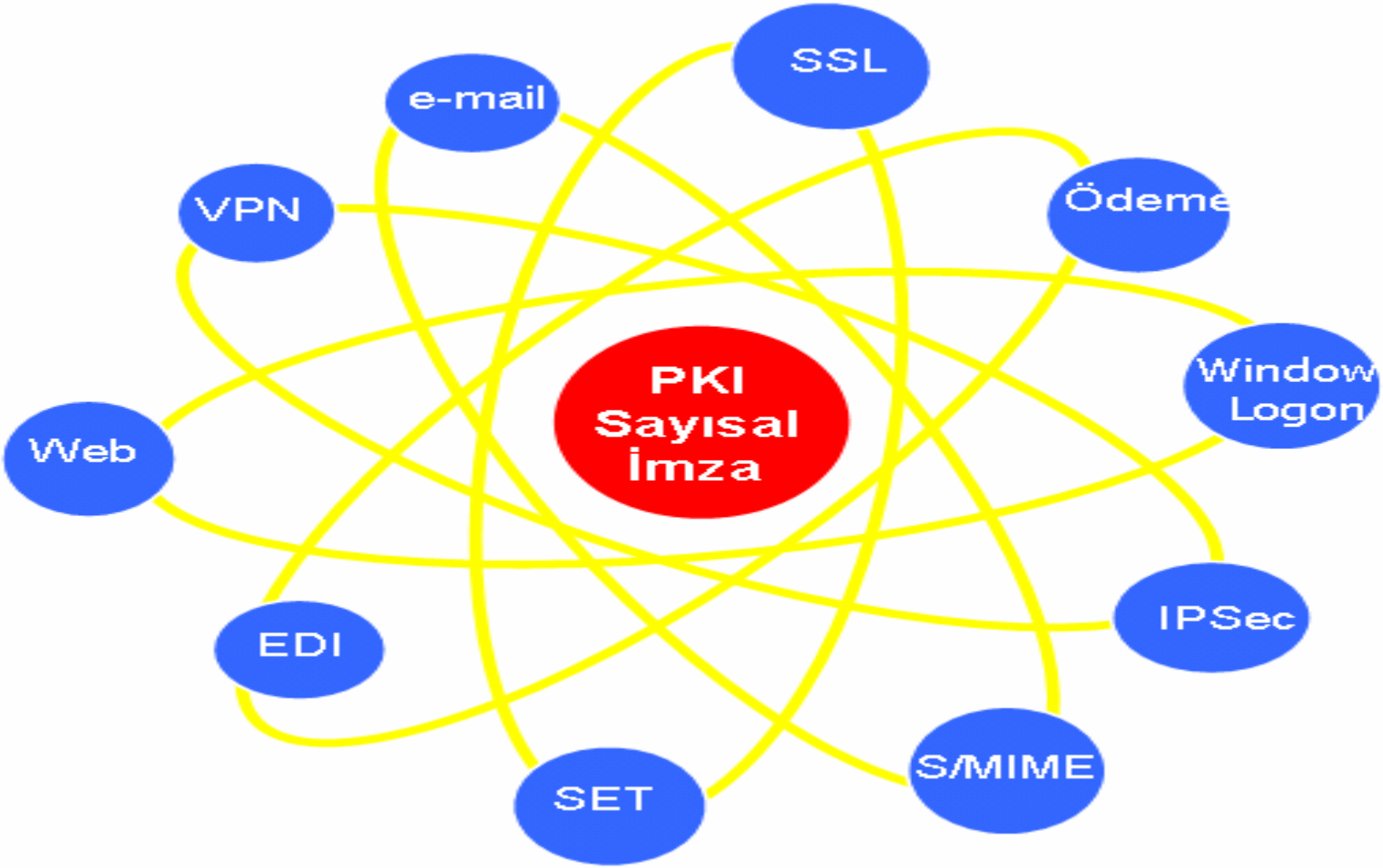
- Giriş
- Temel Kavramlar
- Sayısal (Elektronik) İmza
- Açık Anahtar Altyapısı ile Sayısal İmza Çözümü
- Açık Anahtar Altyapısı Bileşenleri
- Açık Anahtar Altyapısı Mimarileri
- Sonuç

Sonuç

SAYISAL SERTİFİKA KULLANIM ALANLARI

- Sayısal Sertifika Kullanım Alanları [2]:
- Güvenli e-posta haberleşmesi (Secure Multi-Purpose Internet Mail Extensions, S/MIME)
- Bilgisayar ortamında saklanan verilerin imzalı ve şifreli saklanması (Masaüstü Güvenliği/Desktop Security)
- Akıllı Kartla Güvenli Oturum Açma (Windows Logon, Kerberos)
- İmzalı Formlar (Signed Forms)
- Sayısal Noter
- Kod İmzalama
- XML İmzalama
- İnternet protokolü Güvenliği (Internet Protokol Security, IPSEC) [4]
- Taşıma Katmanı Güvenliği (Transport Layer Security, TLS)
- Güvenli Yuvalar Katmanı (Secure Socket Layer, SSL) [3]
- Güvenilir Zaman Damgası (Time Stamp Protocol, TSP) [5]
- Sanal Özel Ağ (Virtual Private Network, VPN) [4]

Sonuç



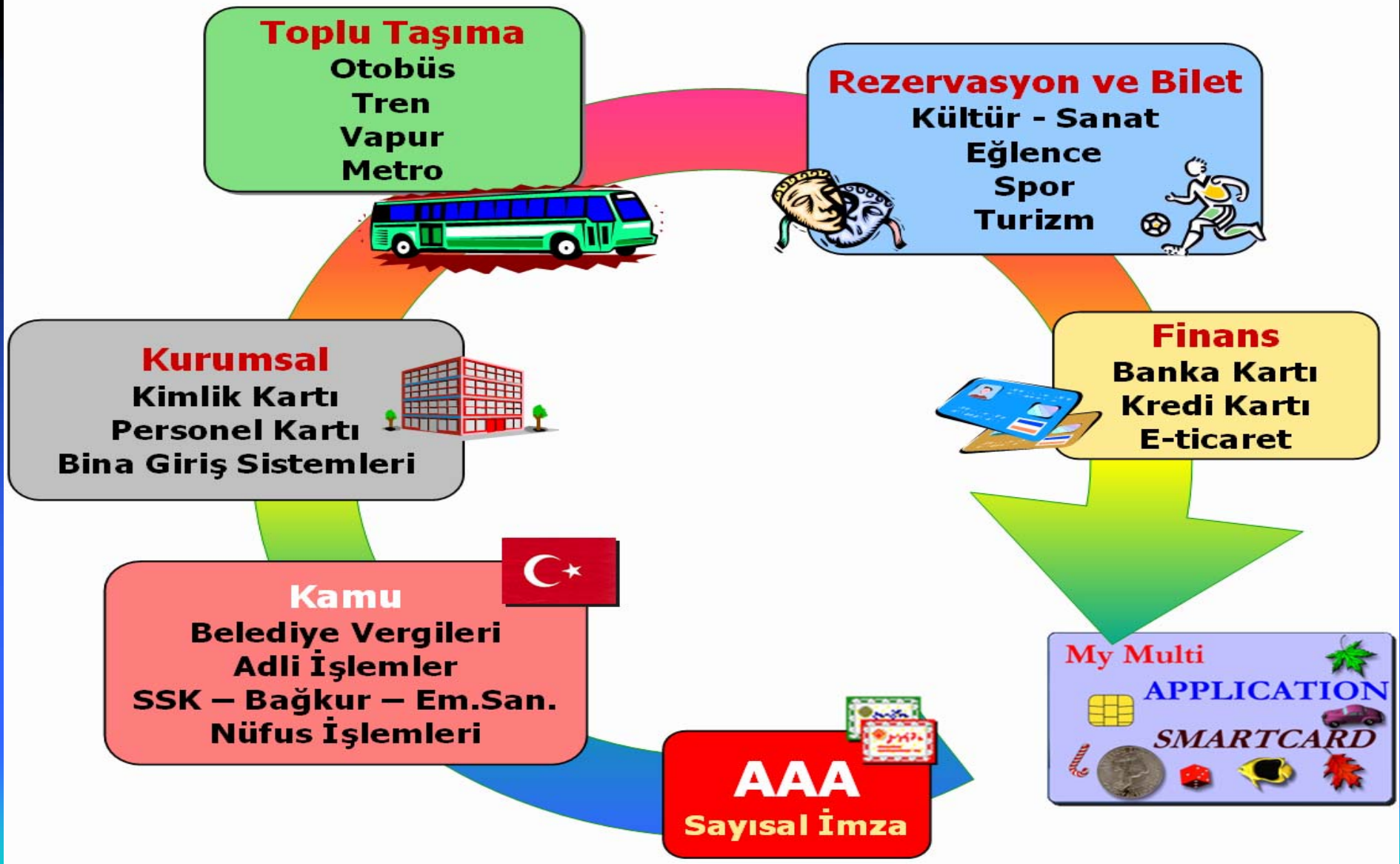
SAYISAL SERTİFİKA KULLANIM ALANLARI

Sonuç

SAYISAL İMZA KANUNU

TBMM Genel Kurulu'nda 15 Ocak 2004 tarihinde kabul edilerek, 23 Ocak 2004 tarihli Resmi Gazete'de (Sayı: 25355) yayımlanan yasa, 23 Temmuz 2004 tarihinde yürürlüğe girdi.

Sonuç


Toplu Taşıma
Otobüs
Tren
Vapur
Metro
Rezervasyon ve Bilet
Kültür - Sanat
Eğlence
Spor
Turizm
Kurumsal
Kimlik Kartı
Personel Kartı
Bina Giriş Sistemleri
Finans
Banka Kartı
Kredi Kartı
E-ticaret
Kamu
Belediye Vergileri
Adli İşlemler
SSK – Bağkur – Em.San.
Nüfus İşlemleri
AAA
Sayısal İmza
My Multi
APPLICATION
SMARTCARD