AAA Temelleri

Emrah DURMAZ

Uzman Araştırmacı
E-Posta: emrah.durmaz@kamusm.gov.tr

TÜBİTAK
KAMU SERTİFİKASYON MERKEZİ

Sunum Planı

- AAA Neden Gereklidir?
- Basit Sertifikalar
- İdeal Sertifika
- Açık Anahtar Sertifikaları
- Sertifika İptal Listeleri
- Çevrimiçi Sertifika Durum Protokolü (OCSP)
- SSL
- Zaman Damgası

AAA Neden gereklidir?

- Asimetrik kriptografi sistemlerinin gerçeklenmesi
- Doğru anahtarların güvenli bir şekilde oluşturulması
- Kimlik doğrulamanın yapılabilmesi
- Sertifikaların hayat döngüsünün idamesi
- Sertifikaların doğrulanması
- Güvenli arşivleme ve anahtar geri kazanımları
- İmza ve zaman damgalarının oluşturulması

Basit Sertifikalar Kartvizit Örneği

- Sertifika kullanarak bir özel anahtarın kime ait olduğunu ispatlayabiliriz.
- Kartvizitleri basit sertifikalar olarak kullanmak mümkündür.
- Bir toplantı yapıldığını ve Ahmet'in herkese kartvizitini dağıttığını düşünelim.

Ön

Zirve Finans

Ahmet Uzun
Yönetici

Zirve İş Merkezi 80120
Mecidiyeköy, İstanbul

Tel: (212) 265 00 00 (PBX)

Arka

Zirve Finans

Ahmet Uzun
Yönetici

E-posta:
auzun@zirve.com.tr

RSA Açık Anahtar:
2489349e894859f454894
50dab45454ca0908d8809

Basit Sertifikalar Kartvizit Örneği

- Ahmet kartvizitin arkasındaki açık anahtara denk gelen özel anahtarın kendisinde olduğunu iddia etmektedir.
- Bu kartı alan Burcu Hanım kartta Ahmet Beyin ismi yazdığı için karttaki açık anahtarın ona ait olduğunu varsayar.
- Burcu Hanım kartı elden alsa bile kartın üzerinde yazan isim ve şirket bilgilerinin doğruluğu şüphelidir.
- Kart üzerindeki bilgilerin güncel olması garanti edilemez.

Basit Sertifikalar Kartvizit Örneği

- Ahmet Bey 1 ay sonra işinden çıkarsa ya da özel anahtarını kaybederse kartviziti geçersiz olacaktır ama bunu kime ve nasıl duyuracaktır?
- Burcu Hanım açık anahtarı eliyle ve hatasız olarak bilgisayarına girmelidir.

Basit Sertifikalar
Kredi Kartı Örneği

- Kart sahibinin adı
- Hesap numarası
- Veren bankanın veya kuruluşun adı
- Son kullanım tarihi
- Fotoğraf, imza ve hologram
- Sadece 2 kişi arasında değil, Visa kabul eden her yerde geçerli
- Bilgiler manyetik bantta saklı

İdeal Sertifika

- İnternette yayınlanabilmesi ve otomatik olarak işlenebilmesi için tamamen sayısal olmalıdır.
- Özel anahtarın sahibinin kimlik bilgilerini içermelidir.
- Ne zaman yayınlandığını ve ne zamana kadar geçerli olduğunu içermelidir.
- Özel anahtarın sahibi tarafından değil güvenilir bir 3. kurum tarafından yaratılmalıdır.

İdeal Sertifika

- Güvenilen kurum birçok sertifika yaratacağı için (aynı kullanıcı için bile birden fazla) her bir sertifikanın diğerinden kolayca ayırt edilebilmesi gereklidir.
- Bir sertifikanın gerçek ya da sahte olduğu kolayca tespit edilebilmelidir.
- Değiştirilmeye karşı korunmuş olmalıdır.
- Hangi uygulamalar için kullanılabileceği sertifikada belirtilmelidir.

Açık Anahtar Sertifikaları

- Sayısaldır, bilgisayarda hazırlanır. (X.509)
- Sahibinin adını ve açık anahtarını 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.

Açık Anahtar Sertifikaları
Örnek Sertifika

Seri No	2368
Sertifika Sahibi	Ahmet Uzun-43657465098
Yayınlayan	KamuSM
Yayın Tarihi	05.02.2010
Son Kullanım	05.02.2013
Açık Anahtar	2489349e894859f45489450dab45454 ca0908d8809

Kamu SM Elektronik İmzası	ae89349c989893e8989548d0 823048b08023f9e903

Sertifika Eklentileri (Extensions)

- Authority Key Identifier
- Subject Key Identifier
- Key Usage
- Certificate Policies
- Policy Mappings
- Subject Alternative Name
- Issuer Alternative Name
- Subject Directory Attributes

Sertifika Eklentileri (Extensions)

- Basic Constraints
- Extended Key Usage
- CRL Distribution Points
- Freshest CRL
- Authority Information Access
- Subject Information Access

Açık Anahtar Sertifikaları

- ✓ Sayısaldır.
- ✓ Sahibi hakkında gerekli bilgileri içerir.
- ✓ Yayın ve son kullanma tarihini içerir.
- ✓ Yayıncısının adını içerir ve onun sayısal imzasıyla doğrulanması yapılır.
- ✓ Yayıncı adı ve sertifika seri numarası sertifikanın tekil olmasını sağlar.

Açık Anahtar Sertifikaları

- ✓ Sertifikanın bütünlüğünün bozulması engellenemez ama böyle bir durum sayısal imzanın kontrol edilmesiyle hemen anlaşılır.
- ? Sertifikanın içindeki bilgilerin güncel olup olmadığından nasıl emin olunacaktır?

Sertifika İptal Listeleri (SİL - CRL)

- Sertifika içeriğinin güncel olup olmadığı sorusuna cevap verir
  - Sertifika sahibi özel anahtarını kaybettiği için yeni bir özel-açık anahtar çifti 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 yayınlanır.

Sertifika İptal Listeleri
Örnek SİL

Yayınlayan	**KamuSM**
Yayın Tarihi	**22.11.2011**
Son Kullanım	**23.11.2011**

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

Kamu SM Sayısal İmzası	6656e345200cde989228d0823aec8b08023f9

Sertifika İptal Nedenleri

- Akıllı kartın kaybedilmesi veya çalınması
- Akıllı kartın erişilemez olması (pin-puk)
- Kullanıcının sertifikada yer alan bilgilerinin değişmesi
- Sertifika Makamı'nın iptal edilmesi!
- Sertifika Makamı'nın anahtarının çalınması!!!

Çevrimiçi Sertifika Durum Protokolü (OCSP)

- SİL'lerin bir periyot boyunca geçerli olması, bu periyot boyunca iptal edilen sertifikalardan kullanıcıların ancak bir sonraki periyotta haberlerinin olmasına yol açmaktadır.
- Çözüm: Çevrimiçi Sertifika Durum Protokolü
  - Her SM'ye ait bir veya birden fazla sertifikalı OCSP sunucusu olabilir. OCSP sunucusu o SM'nin yayınladığı sertifikaların iptal edilip edilmediği bilgisini verir.

Çevrimiçi Sertifika Durum Protokolü (OCSP)

- Kullanıcı isteği: X no'lu sertifikanın durumu nedir?
- OCSP sunucusu yanıtı:
  - İptal edilmemiş
  - İptal edilmiş
    - İptal nedeni
    - İptal zamanı
  - Bilinmiyor

SSL

- Haberleşen iki uygulama arasında sağlanan hizmetler
  - Kimlik doğrulama
  - Bütünlük
  - Gizlilik
- Sunucunun kimliğini istemciye ispat eder
- İstemcinin kimliğini sunucuya ispat eder (seçimlik)

Zaman Damgası (Timestamp)

İmza zamanı olarak aşağıdakilerden birisi belirlenebilir:

- Kullanıcı makinasındaki sistem saati veya kurumdaki bir sunucudan alınan zaman bilgisi
- Zaman Damgası Sunucusundan alınan zaman bilgisi

Zaman Damgası (Timestamp)

- Kullanıcı makinasındaki sistem saati veya kurumdaki bir sunucudan alınan saat bilgisi imza dosyasına eklenebilir. Ancak bu yöntem imza zamanının belirlenmesinde güvenilir kabul edilmemektedir.
- Zaman damgası (Timestamp)
  - İmzanın zaman damgası alındığı tarihten önce oluşturulduğu ispatlanır.
  - Zaman damgası imza dosyasına sonradan eklenir.
    - Kullanıcı imzayı oluşturduktan hemen sonra kullanıcı uygulaması zaman damgası alabilir.
    - Kullanıcı imzalı belgeyi alıcı tarafa gönderdikten sonra alıcı tarafın uygulaması zaman damgası alabilir.