MUH442 Bilişimde Güvenlik – 2

Prof. Dr. Hasan Hüseyin BALIK

(12. Hafta)

İçerik

- 4.Ağ güvenliği
  - 4.1. İnternet Güvenlik Protokolleri ve Standartları
  - 4.2.İnternet Kimlik Doğrulama Uygulamaları
  - 4.3 Kablosuz Ağ Güvenliği

4.2. İnternet Kimlik Doğrulama Uygulamaları

4.2.İçerik

- Kerberos
- X.509
- Açık Anahtar Altyapısı
- Birleşik Kimlik Yönetimi

Kerberos'a Genel Bakış

- Başlangıçta MIT'de geliştirilmiştir
- Hem kamu malı hem de ticari olarak desteklenen sürümlerde kullanılabilen yazılım yardımcı programıdır
- Bir İnternet standardı olarak yayınlanmıştır ve uzaktan kimlik doğrulama için varsayılan standarttır
- Genel şema, güvenilir bir üçüncü taraf kimlik doğrulama hizmetidir
- Bir kullanıcının çağrılan her hizmet için kimliğini kanıtlamasını gerektirir ve sunucuların kimliklerini istemcilere kanıtlamasını gerektirir

Kerberos Protokolü

İstemcileri, uygulama sunucularını ve bir Kerberos sunucusunu içerir

- Bir istemci/sunucu diyaloğunun güvenliğine yönelik çeşitli tehditlere karşı koymak için tasarlanmıştır
- Açık güvenlik riski kimliğe bürünmedir
- Sunucular, hizmet talep eden istemcilerin/kullanıcıların kimliklerini doğrulayabilmelidir

Kimlik Doğrulama Sunucusu (AS) kullanır

- Kullanıcı başlangıçta kimlik doğrulaması için AS ile görüşür
- AS, kimliği doğrular ve ardından bilgileri, daha sonra istemciden gelen hizmet isteklerini kabul edecek olan bir uygulama sunucusuna iletir

Bunu güvenli bir şekilde yapmanın bir yolunu bulmak gerekir

- İstemci, kullanıcının parolasını ağ üzerinden AS'ye gönderirse, bir saldırganın parolayı gözlemleyebilir
- Bir saldırgan AS'yi taklit edebilir ve yanlış bir doğrulama gönderebilir

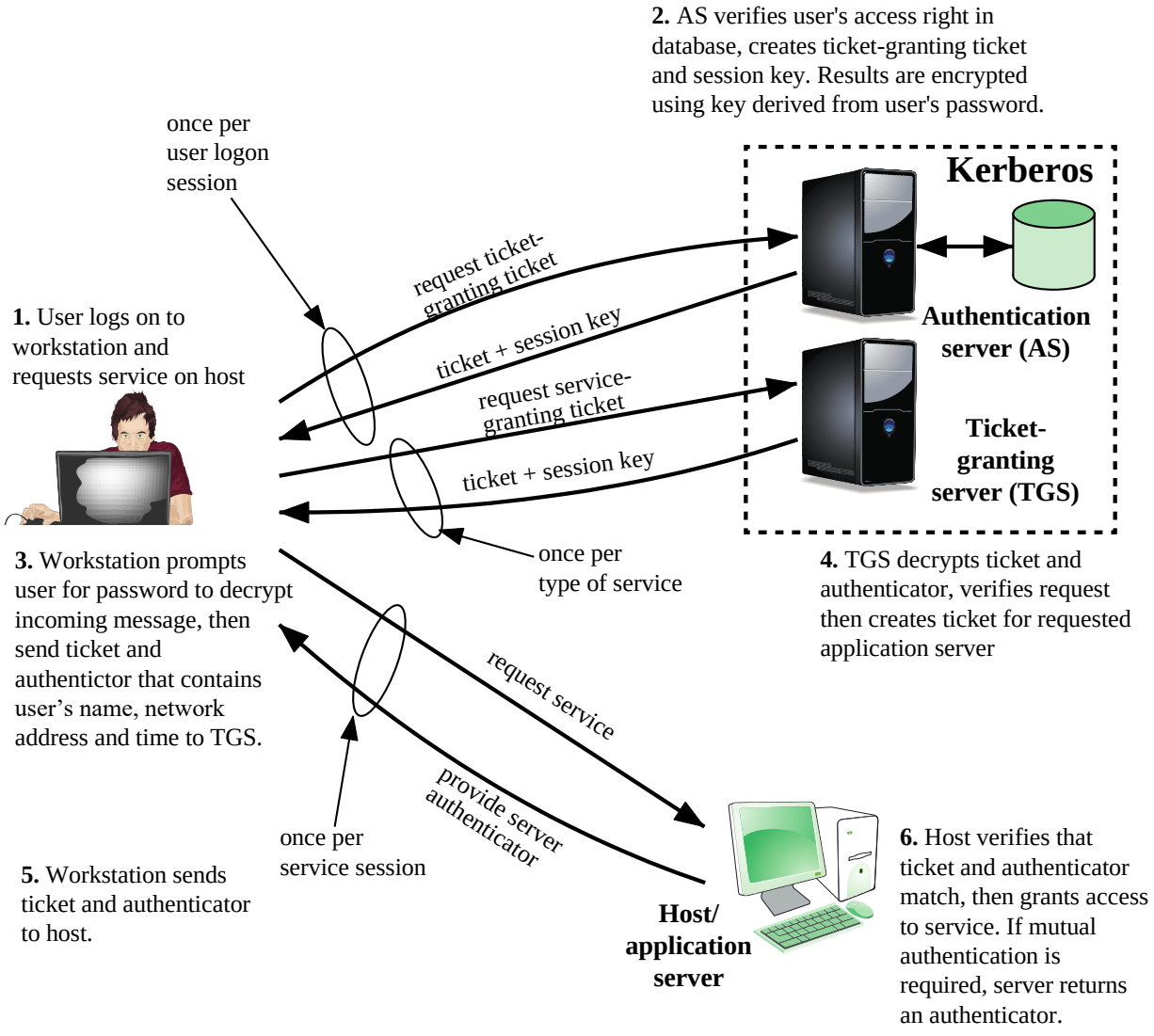

Figure 23.1 Overview of Kerberos

Kerberos Alemleri (Realms)

- Bir Kerberos ortamı şunlardan oluşur:
  - Bir Kerberos sunucusu
  - Hepsi sunucuya kayıtlı bir dizi istemci
  - Anahtarları sunucuyla paylaşan bir dizi uygulama sunucusu
- Böyle bir ortama alem (realm) denir
  - Farklı idari organizasyonlar altındaki istemci ve sunucu ağları genellikle farklı alemler oluşturur.
- Birden fazla alem varsa:
  - Kerberos sunucuları, gizli bir anahtarı paylaşmalı ve kullanıcılarının kimliğini doğrulamak için diğer alemdeki Kerberos sunucusuna güvenmelidir.
  - İkinci alemdeki katılımcı sunucular da birinci alemdeki Kerberos sunucusuna güvenmeye istekli olmalıdır.

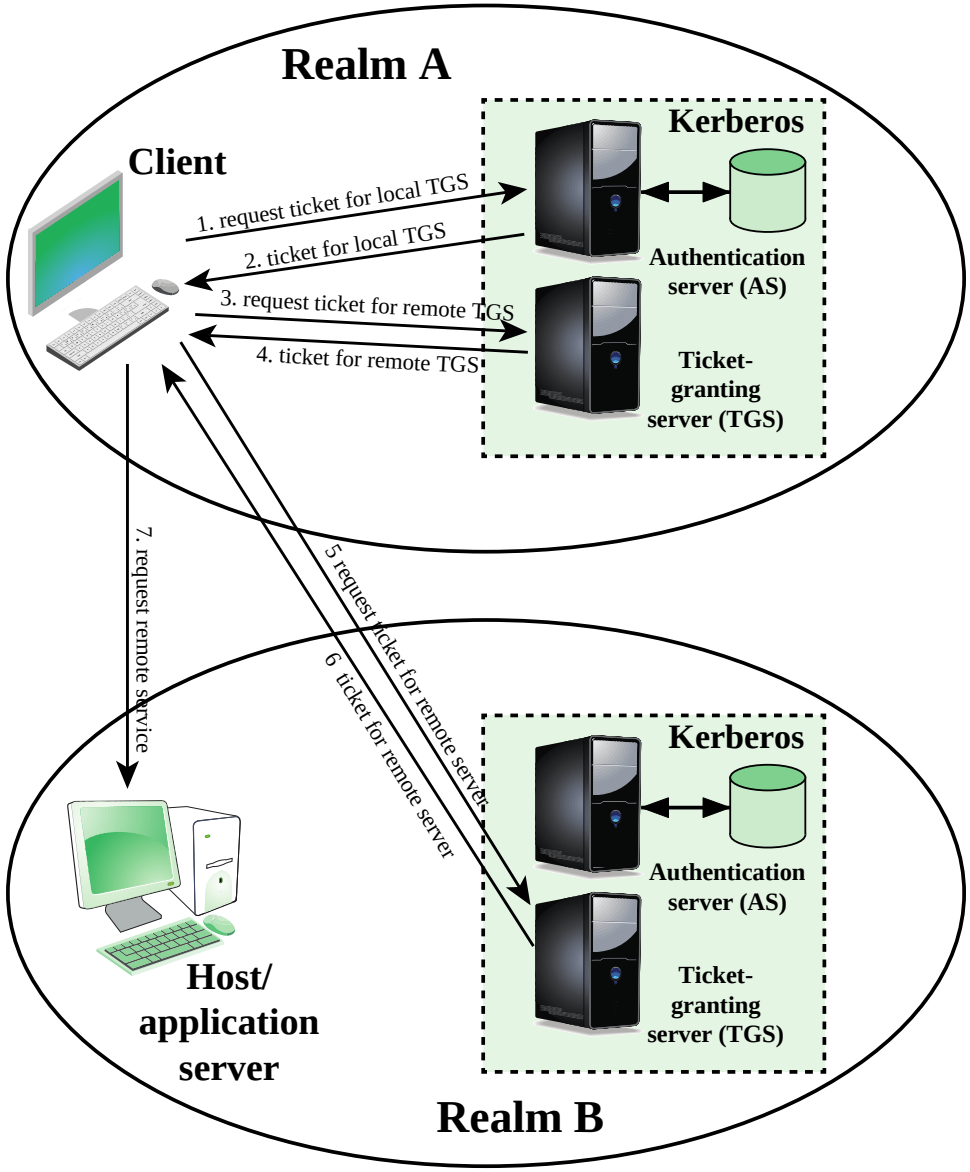

Figure 23.2 Request for Service in Another Realm

Kerberos Sürüm 4 ve 5

- Yaygın olarak kullanılan ilk Kerberos sürümü, 1980'lerin sonunda yayınlanan 4. sürümdür.
- Sürüm 5 1993'de piyasaya sürüldü ve 2005'de güncellendi
- Microsoft'un Active Directory ve UNIX/Linux ve Mac OS X'de uygulanmaktadır
- Sürüm 5'te bulunan iyileştirmeler:
  - Şifreli bir mesaj, bir şifreleme algoritması tanımlayıcısı ile etiketlenir
    - Bu, kullanıcıların Kerberos'u DES dışında bir algoritma kullanacak şekilde yapılandırmasını sağlar.
  - Kimlik doğrulama iletimini destekler
    - Bir istemcinin bir sunucuya erişmesini ve o sunucunun istemci adına başka bir sunucuya erişmesini sağlar
    - Sürüm 4'e göre daha az güvenli anahtar değişimi gerektiren alemler arası kimlik doğrulama yöntemini destekler

Kerberos Performans Sorunları

Daha büyük istemci-sunucu kurulumları

Sistem uygun şekilde yapılandırılmışsa, büyük ölçekli bir ortamda çok az performans etkisi

Kerberos güvenliği, Kerberos sunucusunu ayrı, izole bir makineye yerleştirerek en iyi şekilde sağlanır

Birden fazla alem için motivasyon performansla ilgili değil idaridir

Sertifika Yetkilisi (CA)

Sertifika şunlardan oluşur:

- Anahtar sahibinin kimliğine sahip bir açık/genel anahtar
- Güvenilir bir üçüncü şahıs tarafından onaylama.
- Tipik olarak üçüncü taraf, kullanıcı topluluğu tarafından güvenilen bir CA'dır (devlet kurumu, telekomünikasyon şirketi, finans kurumu veya diğer güvenilir zirve kuruluş gibi)

Kullanıcı, açık anahtarını yetkiliye güvenli bir şekilde sunabilir ve sertifika alabilir

- Kullanıcı daha sonra sertifikayı yayınlayabilir veya başkalarına gönderebilir
- Bu kullanıcının genel/açık anahtarına ihtiyaç duyan herkes, sertifikayı alabilir ve ekteki güvenilir imza yoluyla geçerli olduğunu doğrulayabilir

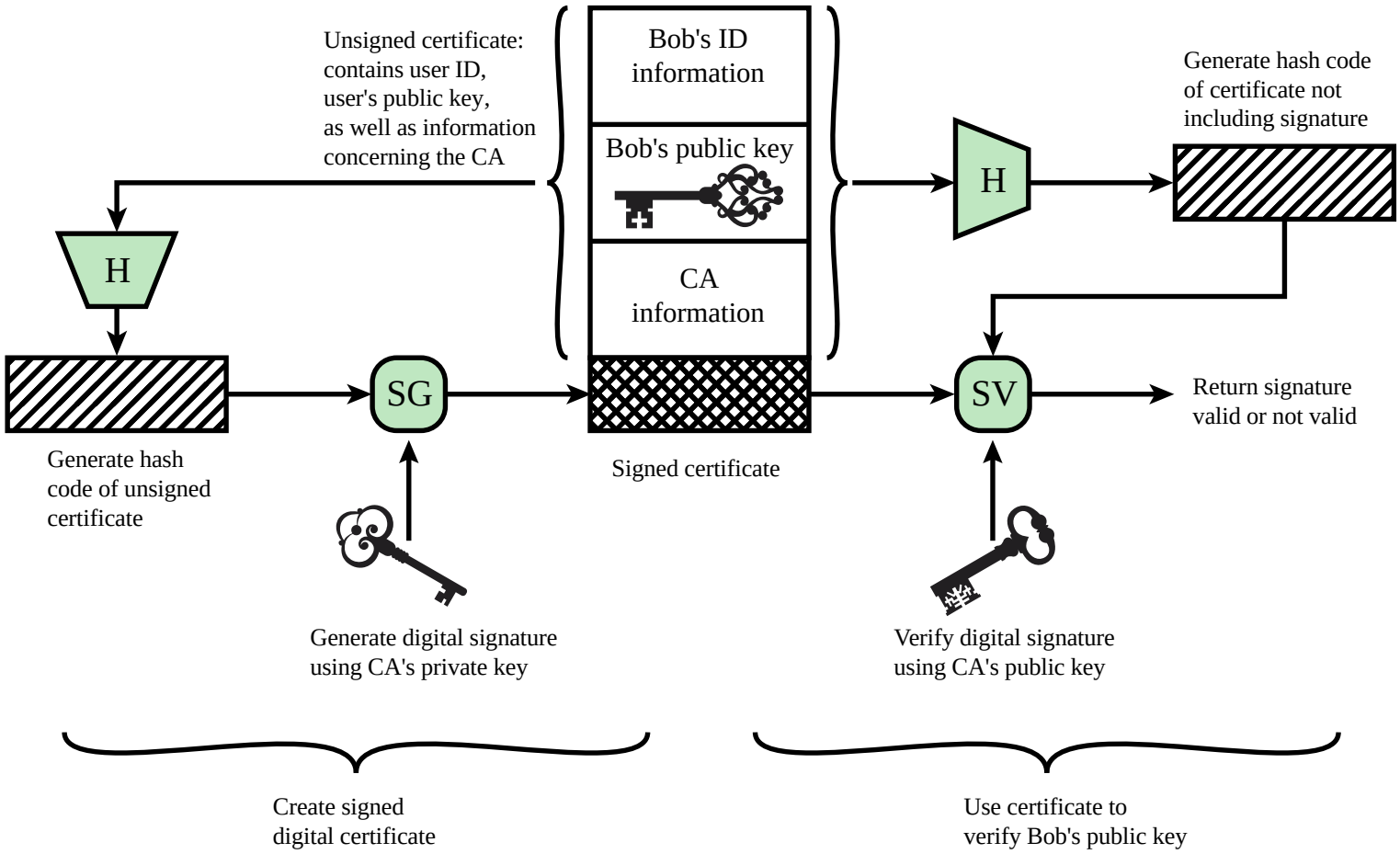

Figure 2.8 Public-Key Certificate Use

X.509

- RFC 5280 (Internet X.509 Ortak Anahtar Altyapısı Sertifikası ve Sertifika İptal Listesi (CRL) Profili, 2008) ’de tanımlanmıştır
- Açık/genel anahtar sertifikaları için en yaygın kabul gören formatıdır
- Sertifikalar, aşağıdakiler de dahil olmak üzere çoğu ağ güvenliği uygulamasında kullanılır:
  - IP güvenliği (IPSEC)
  - Güvenli soket katmanı (SSL)
  - Güvenli elektronik işlemler (SET)
  - S/MIME
  - eTicaret uygulamaları

Belirli öğe değerleri veya belirli uzantıların varlığı ile ayırt edilen bir dizi özel varyant da mevcuttur:

- Geleneksel (uzun ömürlü) sertifikalar
  - CA ve "son kullanıcı" sertifikaları
  - Tipik olarak aylar ve yıllar arasındaki geçerlilik süreleri için verilir
- Kısa ömürlü sertifikalar
  - Geleneksel sertifikaların bazı ek yüklerinden ve sınırlamalarından kaçınırken, grid bilgi işlem gibi uygulamalar için kimlik doğrulama sağlamak için kullanılır
  - Saatlerden günlere kadar geçerlilik süreleri vardır, bu da tehlikeye atılırsa kötüye kullanım süresini sınırlar.
  - Genellikle tanınan CA'lar tarafından verilmediğinden, bunları veren kuruluşun dışında doğrulamayla ilgili sorunlar vardır.
- Proxy sertifikaları
  - Kısa ömürlü sertifikaların bazı sınırlamalarını ele alırken, grid bilgi işlem gibi uygulamalar için kimlik doğrulama sağlamak için yaygın olarak kullanılır.
  - RFC 3820'de tanımlanmıştır
  - "Proxy sertifikası" uzantısının varlığıyla tanımlanır
  - Bir "son kullanıcı" sertifikasının başka bir sertifikayı imzalamasına izin verirler.
  - Bir kullanıcının, tam sertifikasını ve hakkını sağlaması gerekmeden, bazı ortamlardaki kaynaklara erişmek için kolayca bir kimlik bilgisi oluşturmasına izin verin
- Öznitelik sertifikaları
  - RFC 5755'te tanımlanmıştır
  - Bir kullanıcının kimliğini genellikle yetkilendirme ve erişim kontrolü için kullanılan bir dizi özniteliğe bağlamak için farklı bir sertifika biçimi kullanır
  - Bir kullanıcı, farklı amaçlar için farklı nitelikler kümesine sahip bir dizi farklı nitelik sertifikasına sahip olabilir.
  - Bir "Nitelikler" uzantısında tanımlıdır

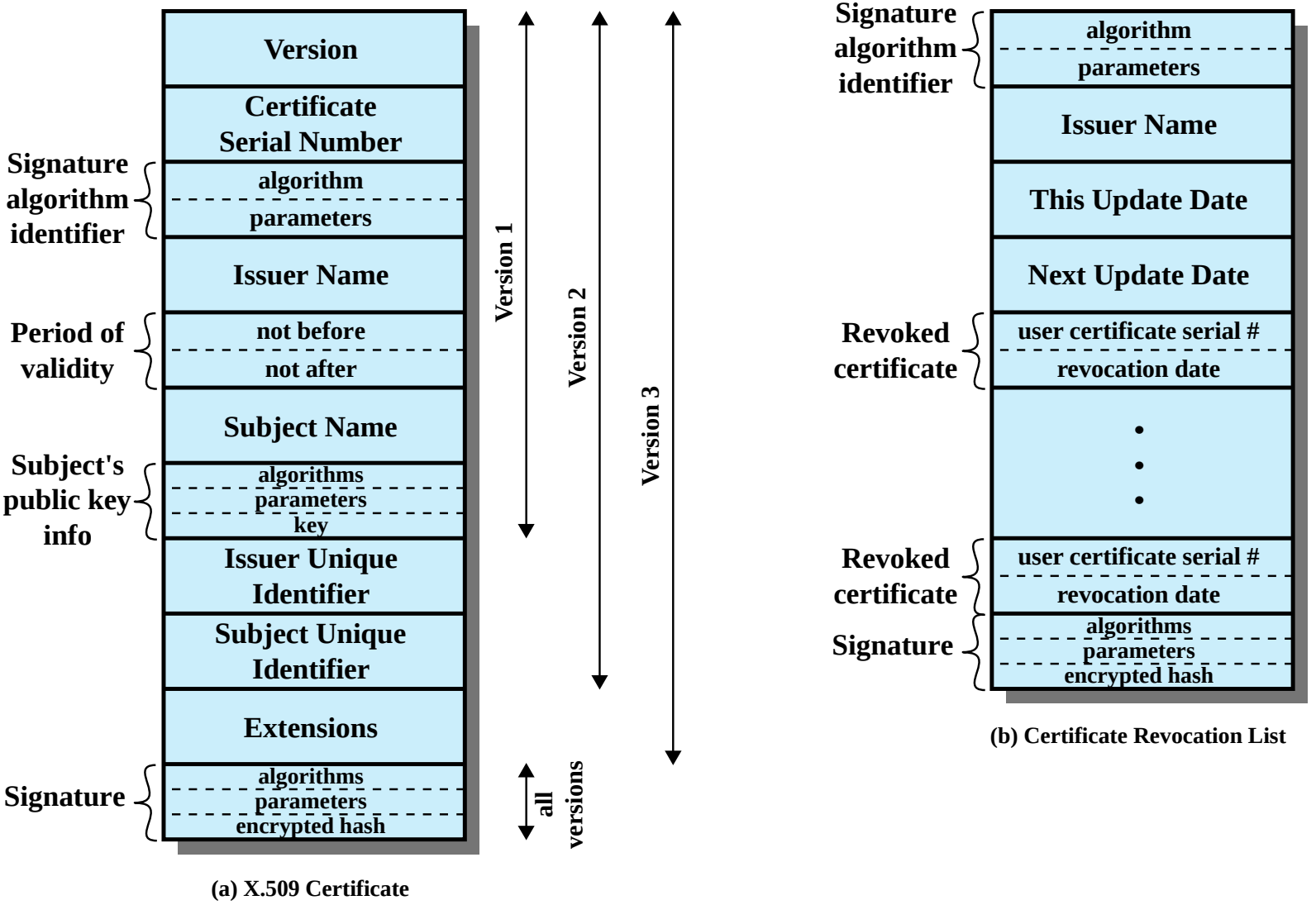

Figure 23.3 X.509 Formats

- X.509 standardı, Şekil 23.3b'de gösterilen unsurları içeren, veren tarafından imzalanmış bir sertifika iptal listesi (CRL) tanımlar
- İptal edilen her sertifika girişi, bir sertifikanın seri numarasını ve o sertifikanın iptal tarihini içerir. Seri numaraları bir CA içinde benzersiz olduğundan yeterlidir.
- Bir uygulama bir sertifika aldığında, X.509 standardı, sertifikayı veren CA için geçerli CRL'yi kontrol ederek sertifikanın iptal edilip edilmediğini belirlemesi gerekir.
- CA belirli bir sertifikanın geçerli olup olmadığını sorgulamak için RFC 6960'ı (X.509 İnternet Genel Anahtar Altyapısı Çevrimiçi Sertifika Durum Protokolü - OCSP, 2013) kullanmaktır.
- Başlangıçta çoğu X.509 sertifikası, içeriklerinin bir MD5 özeti ile imzalamıştır
- 2000'lerde MD5 yerine SHA-1 hash algoritması önerildi.
- 2017'nin başlarından itibaren çoğu tarayıcı artık SHA-1 veya MD5 kullanan sertifikaları reddetmekte yerine SHA-2 algoritmasını desteklemektedir.
- Yakın gelecekte bir alternatif olarak SHA-3 desteği olacaktır.

Açık Anahtar Altyapısı (PKI)

- RFC 4949 (İnternet Güvenlik Sözlüğü, Sürüm 2, 2007)'de tanımlanmıştır
- Asimetrik şifrelemeye dayalı dijital sertifikaları oluşturmak, yönetmek, depolamak, dağıtmak ve iptal etmek için gereken donanım, yazılım, kişiler, politikalar ve prosedürler kümesidir
- Genel anahtarların güvenli, rahat ve verimli bir şekilde edinilmesini sağlamak için geliştirilmiştir
- "Güven mağazası / Trust Store"
  - CA'ların ve ortak anahtarlarının bir listesi

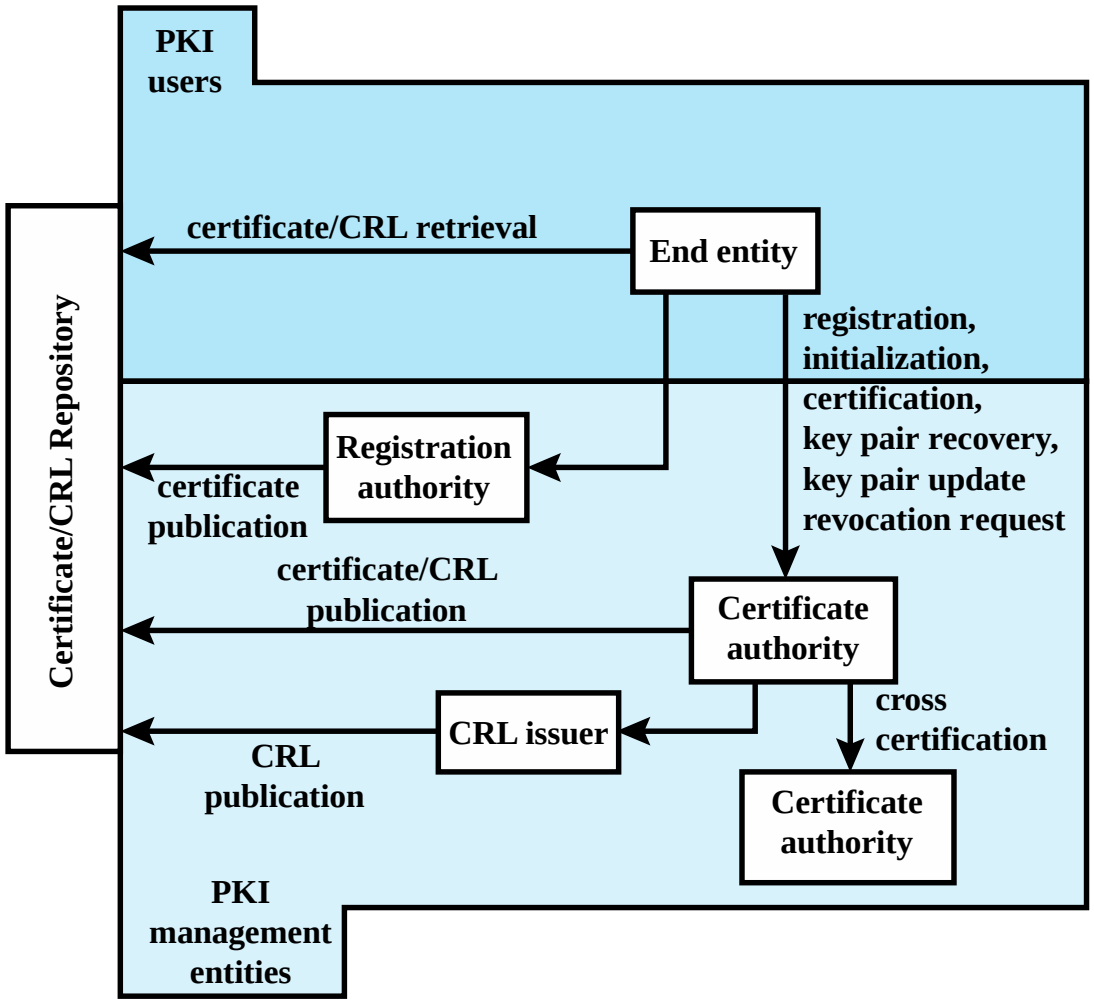

Figure 23.4 PKIX Architectural Model