Kriptográfia

Tizenkettedik előadás
X.509 tanúsítványok

Németh L. Zoltán
SZTE, Számítástudomány Alapjai Tanszék
2007 ősz

X.509 Hitelesítési szolgáltatások
X.509 Authentication Service

- része part az ITU-T (*International Telecommunication Union Telecommunication Standardization Sector*) X.500-as katalógus szolgáltatások (directory service) szabványának.
  - X.500: hogyan tároljunk (osztott) szervereken adatbázist a felhasználók adatairól
- hitelesítési szolgáltatásokhoz biztosít keretetrendszert
- a katalógusban **nyilvános kulcs tanúsítványokat** (public-key certificates) tárolhatunk, azaz a nyilvános kulcs hitelességét egy hitelesítés szolgáltató (certification authority, CA) aláírása igazolhatja.
- hitelesítési protokollokat is definiál:
  - egy utas (one-way)
  - két utas (two-way) és
  - három utas (tree-way) autentikációt.

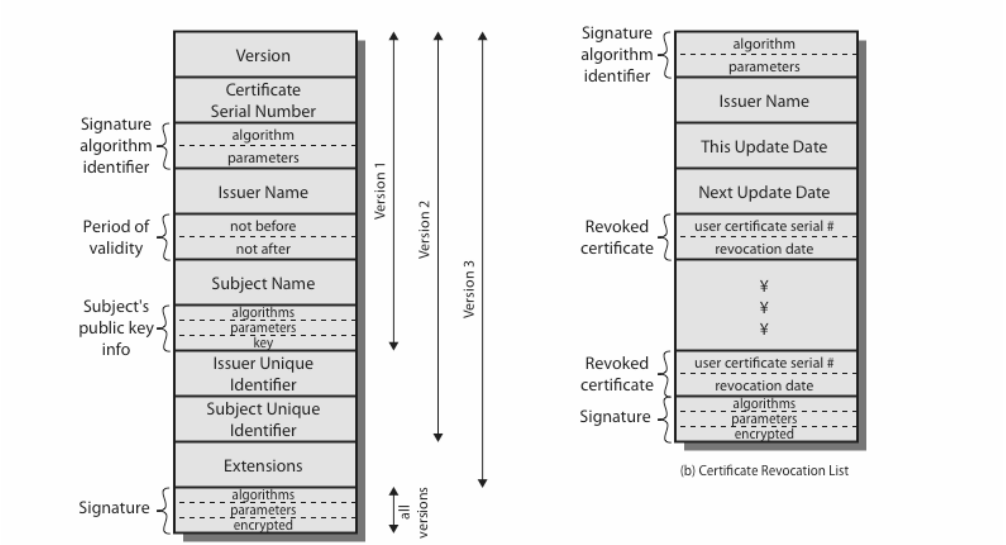
X.509 Hitelesítési szolgáltatások
X.509 Authentication Service

- a megvalósítás alapja a
  - nyilvános kulcsú titkosítás
  - és a digitális aláírások
- egyetlen algoritmust sem köt ki a szabvány, de az RSA-t javasolja
- az X.509 tanúsítványok széles körben elterjedtek:
  - HTTPS
  - S/MIME (Secure Multipurpose Internet Mail Extensions)
  - IPSec
  - SSL/TLS
  - SET (Secure Electronic Transaction)

Az X.509 tanúsítványok adatai

- V, version: verzió szám (1, 2, vagy 3)
- SN, serial number: sorszám egyedi (a CA-n belül), azonosítja a tanúsítványt
- Signature Algorithm: az aláíró algoritmus azonosítója a
- Issuer: kibocsátó CA neve (X.500 szerint)
- Validity: érvényességi idő, tól – ig dátum
- Subject: a tanúsítvány alanya, azaz a tulajdonos (X.500) neve
- Subject Public Key Info: az alany nyilvános kulcsának adatai (algoritmus, paraméterek, maga a kulcs)
- Issuer unique identifier: opcionális, csak a v2-től
- Subject unique identifier: opcionális, csak a v2-től
- Extension fields: kiterjesztések, csak v3-ban
- Signature: a többi mező hash értékének az aláírása

Az X.509 tanúsítványok és a visszavonási listák (Revocation Lists) mezői



Példa egy X.509 tanúsítványra, amit maga a kibocsátó írt alá:

Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com
Validity:
    Not Before: Aug 1 00:00:00 1996 GMT
    Not After : Dec 31 23:59:59 2020 GMT
Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc, OU=Certification Services Division, CN=Thawte Server CA/emailAddress=server-certs@thawte.com
Subject Public Key Info: Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
    Modulus (1024 bit): 00:d3: … :87:0d
    Exponent: 65537 (0x10001)
X509v3 extensions:
    X509v3 Basic Constraints:
        critical
        CA:TRUE
Signature Algorithm: md5WithRSAEncryption 07:fa: … 70:47

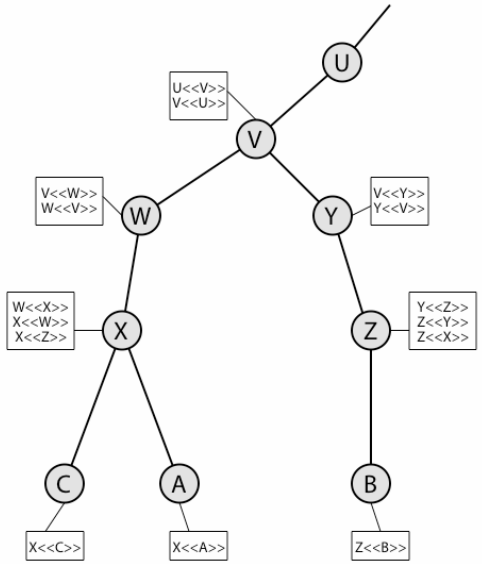
Hogyan juthatunk valakinek a tanusítványhoz?

- a hitelesítés szolgáltató feladata ellenőrizni a hitelesítésért hozzá forduló felhasználók azonosságát
- miután hitelesítette őket tanúsítványt bocsát ki az ellenőrzött adatok és a nyilvános kulcs összetartozásáról
- a tanúsítványt mindenki ellenőrizni tudja, aki hozzáfér a CA nyilvános kulcsához
- mivel csak a CA tud a magánkulcsával aláírni csak ő tud a nyilvános kulcsával ellenőrizhető tanúsítványt kibocsátani
- ezért ha az ellenőrzés sikeres, a tanúsítvány igazolja a benne foglalt nyilvános kulcs hitelességét
- mivel a tanúsítványt nem lehet hamisítani, azokat bátran tárolhatjuk egy publikus katalógusban, vagy elküldhetjük titkosítéás nélkül is

CA hierarchia

- ha a kommunikáló feleknek ugyanaz a hitelsítés szolgáltatójuk (és feltételezük, hogy a CA-juk nyilvános kulcsában biztosak), akkor tudják egymás tanúsítványait ellenőrizni
- de sok felhasználó esetén egyetlen CA nem praktikus
- ezért a CA-knak hierarhikus rendben egymást kell hitelesíteniük. Minden CA
  - hitelesíti a kliensit/leszármazottait (forward certification)
  - és az ősét (backward certification)
- minden kliensnek meg kell bíznia az ősének tanúsítványaiban
- így lehetővé válik bármely CA felhesználó számára minden ugyanabban a hiererchiában szereplő CA tanúsítványának az ellenőrzésére
- Jelölés: `CA<<A>>` jelölje A-nak a CA által aláírt tanúsítványát

A CA hierarchia használata



A az alábbi lánc szerint ellenőrziheti B tanúsítványát:
X<<W>> W<<V>> V<<Y>> Y<<Z>> Z<<B>>

Tanúsítvány visszavonás Certificate Revocation

- a tanúsítványoknak meghatározott érvényességi idejük van
- de szükség lehet ennél korábbi visszavonásukra, pl. ha
  - a felhasználó magánkulcsa kompromittálódott vagy elveszett
  - a felhasználót, már nem hitelesíti az adott CA
  - a CA tanúsítványai kompromittálódtak
- Minden CA egy listát köteles vezetni az általa kiadott, érvényességük lejárta előtt visszavont tanúsítványokról:
  - ez a CA tanúsítvány visszavonási listája (**Certificate Revocation List , CRL**)
- a tanúsítvány ellenőrzéséhez, annak a CA tanúsítvány visszavonási listájával való összevetése is hozzátartozik!

X.509 hitelesítési eljárások (Authentication Procedures)

- Az X.509 három alternatív hitelesítési eljárást is kínál, ezek:
  - Egy utas hitelesítés (One-Way Authentication)
  - Két utas hitelesítés (Two-Way Authentication)
  - Három utas hitelesítés (Three-Way Authentication)
- mind a nyilvános kulcsú aláírásokon (public-key signatures) alapszanak

Egy utas autentikáció

- 1 db üzenet: (**A->B**) melyben ellenőrizhető:
  - A identitása, és hogy valóban **A** feladó
  - az üzenet címzettje valóban **B**
  - az üzenet integritása és eredetisége (azaz nem visszajátszás)
- az üzenetben szereplni kell:
  - egy időbélyegnek: $\mathbf{t_A}$,
  - egy nonce-nak: $\mathbf{r_A}$,
  - **B** azonosítójának: $\mathbf{ID_B}$,
  - melyeket **A** ír alá
- az üzenetben további info is küldhető **B**-nek
  - pl. egy kapcsolatkulcs $\mathbf{K_{ab}}$(persze titkosítva)

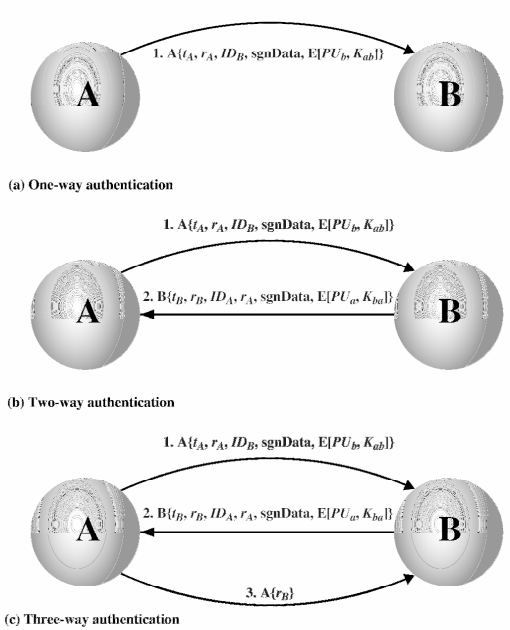
Két utas autentikáció

- 2 db üzenet (**A->B** és **B->A**) mely az előzőn túl biztosítja:
  - **B** identitását, és hogy a válasz **B**-től jött
  - a válasz címzettje valóvan **A**
  - a válasz integritását és eredetiségét
- a válasz (**B->A**) tartalmazza az
  - **A** előző nonce-ját: $\mathbf{r_A}$
  - egy időbélyeget: $\mathbf{t_B}$
  - A azonosítóját: $\mathbf{ID_A}$
  - és egy másik nonce-ot B-től: $\mathbf{r_B}$
- és még más is lehet a válaszban pl: $\mathbf{K_{ba}}$

Három utas autentikáció

- 3 üzenet (A->B, B->A, A->B) melyek kölcsönös hitelesítést biztosítanak szinkronizált órák nélkül
- a két utas autentikáció és még
- egy A-> B üzenet, melyben
  - A visszaküldi B-nek az $\mathbf{r_B}$ nonce-ot aláírva
- így nem kell az időbéylegeket ellenőrizni, vagy bennük megbízni
- a kibocsátott nonce-ok ellenőrzésével a visszajátszás kivédhető

X.509 autentikáviós eljárások



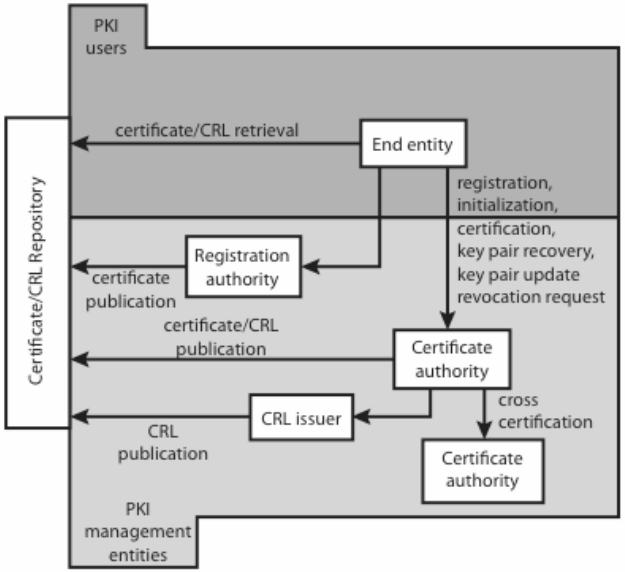
X.509 3. verzió

- a gyakorlat során felismerték, hogy a tanúsítványban több adatot is rögzíteni kell, pl.
  - email/URL, hézirend részletek (policy details), felhasználhatósági megszorítások (usage constraints)
- de ahelyett, hogy konkrétan elneznénk a használható új mezőket célszerűnbb általánosan **kiterjesztésként** (extension) definiálni őket
- egy kiterjesztés az alábbiakból áll:
  - a kiterjesztés azonosítója (extension identifier)
  - a kritikusság indikátor (criticality indicator)
    Ha egy kiterjesztés kritikus, akkor az azt nem ismerő protokollok sem fogadhatják el a tanúsítványt!
  - a kiterjesztés értéke (extension value)

Néhány fontos tanúsítvány kiterjesztés

- kulcs és házirend információk
  - pl. a kulcs azonosítója (több kulcsa lehet egy felhasználónak vagy CA-nak, a magánkulcs hamarabb lejárhat stb.)
  - a házirend mondja meg, hogy a kulcs mire használható, pl.
    - csak adott összegnél kisebb vásárlás esetén fogadható el,
    - csak e-mail aláírására jó,
    - szoftver hitelesítésére is alkalmas, stb.
- a tanúsítvány alanyának és kibocsátójának jellemzői
  - alternatív nevek támogatása, beosztás, más formátumok stb.
- a tanúsítvány út korlátozások
  - korlátozások, melyekkel egy CA egy másik CA tanúsítványait használhatja
  - pl. a legyegyszerűbb extension mező, hogy a tanúsítvány birtokosa CA-e vagy sem (ez kritikus mező)

PKI, Public Key Infrastructure a PKIX modell



Hogyan szerezhetsz saját X.509 tanúsítványt?

- a hitelesség szolgáltatóra azért van szükség, hogy valóban felelősséget is vállaljon az általa történt hitelesítésekért
- ezért a hitelesítés általában a tanúsítvány hatáskörétől függően pénzbe kerül
- Magyarországon a hitelesítés szolgáltatók felügyeletét a
- Nemzeti Hírközlési Hatóság látja el, webhelyén www.nhh.hu megtalálható valamennyi Magyarországon bejegyzett, tanúsítvány kiadásával foglalkozó cég fontosabb adata.
- Avagy ingyenes tanúsítvány igényelhető a CaCert-től: www.cacert.org
  az e-mail címedet tudod hitelesíteni, majd már hitelesített személyek személyes találkozás során, 2 igazolvány alapján rendelhetik a nevedet is a tanúsítványhoz

Felhasznált irodalom

- William Stallings: Cryptography and Network Security, 4th Edition, Prentice Hall, 2006. (Chapter 14)
- Lawrie Brown előadás fóliái (Chapter 14)
- **KIKERES Fogalomtár** 3.0 www.fogalomtar.hu