Authenticiteit: toepassingen

We bespreken 2 manieren om op applicatieniveau authenticering mogelijk te maken:

- Kerberos
- X.509 - PKI

Kerberos

- hond met drie koppen
- bewaakt poort tot de onderwereld
- moderne versie bewaakt toegang tot netwerk
- drie componenten:
  - authenticering
  - gebruikersbeheer
  - audit
- ontwikkeld op MIT samen met IBM en DEC (Athena)
- nu gebruikt in Windows

Kerberos: opzet

- gebruikers op werkstations
- willen toegang tot diensten op servers
- servers verlenen toegang
  - alleen aan welbepaalde gebruikers
  - als authenticiteit van aanvraag na te gaan is

- vraag: hoe **gebruiker** identificeren?
  dmv van werkstation?
- bedreigingen:
  - inbraak in werkstation
  - netwerkadres veranderen
  - luistervinken

Kerberos: opzet (2)

- 1 extra server
  - authenticeert gebruiker t.o.v. server die diensten levert
  - authenticeert server die diensten levert t.o.v. gebruiker
- uitsluitend conventionele encryptie
- versie 4 (1992) en versie 5 (1993, RFC-1510)

- Ontwerpvereisten:
  - veilig (snooping)
  - betrouwbaar (uitvallen server, back-upserver, gedistribueerd)
  - transparant voor gebruiker
  - schaalbaar (veel gebruikers en servers)
  - intypen van wachtwoorden minimaliseren

Kerberos: architectuur

- realm (uitspraak [relm] , betekenis: koninkrijk)
- client – server model
- principals (hoofd, hoofdrolspeler)
  - gebruiker
  - toepassing
  - cliëntcomputer
  - server
  - (netwerk)dienst
- identificatie : uniek door
  - naam
  - instance-naam (is server indien dienst, is rol indien gebruiker)
  - realm
  - vb. rlogin@gonzo.hogent.be

Kerberos: architectuur (2)

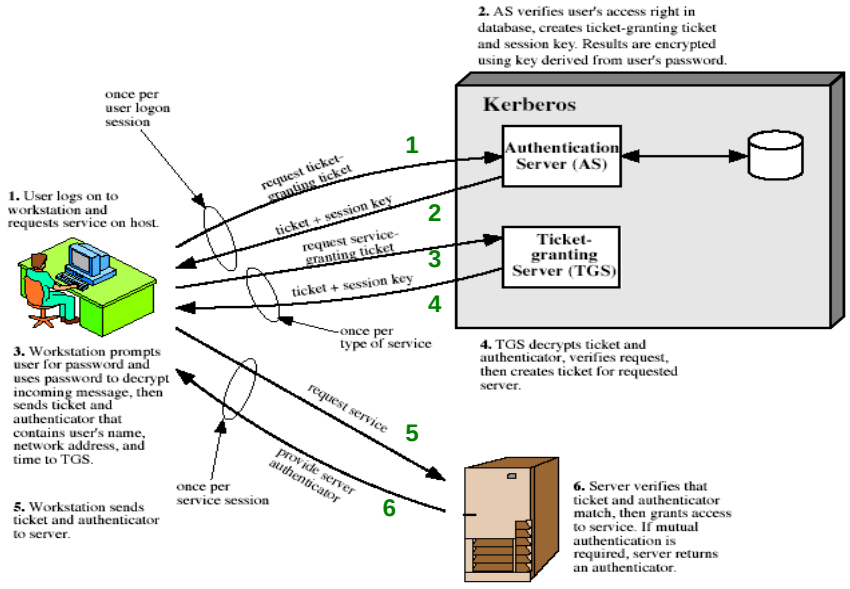
- doel
  - cliëntcomputer authenticeert zich t.o.v. toepassing op server
  - in opdracht van gebruiker
  - zonder uitwisseling van bruikbare gegevens
- derde vertrouwde partij: KDC
- KDC:
  - AS authenticatieserver
  - TGS ticket granting server(s) (grant = verlenen)
- KDC in praktijk
  - 1 of 2 servers
  - 2 diensten
  - fysisch veilig

Kerberos: KDC

- AS bevat voor elke principal in realm
  - naam (user-id, dienst, …)
  - sleutel, wachtwoord indien gebruiker
  - vervaldatum van entry
  - levensduur van tickets
- sleutel geëncrypteerd opgeslagen met hoofdsleutel van KDC
- hoofdsleutel van KDC geheim, apart beheerd
- laat toe database over netwerk te multipliceren

Kerberos - X509 - PKI 7

Kerberos: overzicht protocol



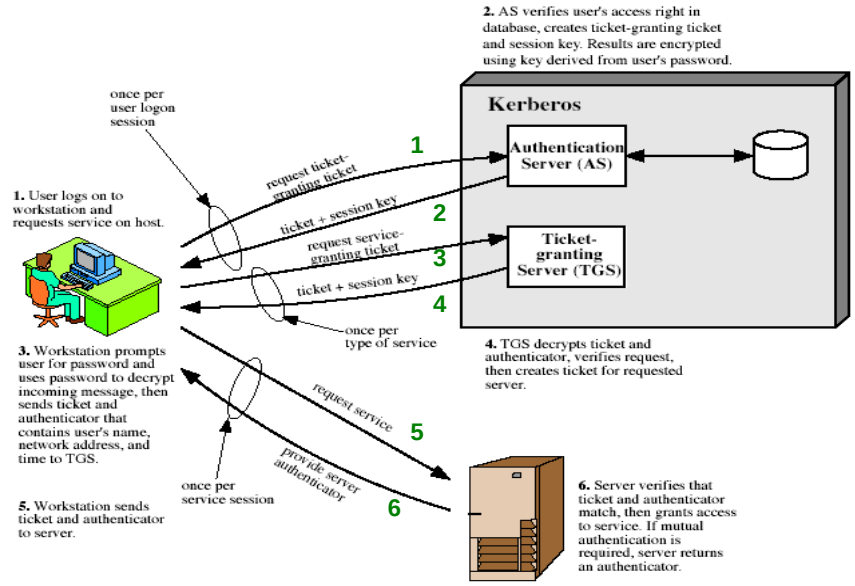
Kerberos: uitgangspunt protocol

- clientcomputer werkt in opdracht van gebruiker
- client wenst diensten van server
- client moet zijn authenticiteit t.o.v. server bewijzen
- KDC geeft geloofwaardigheid van client t.o.v. server
- geen sleuteluitwisseling vooraf tussen client en server

Kerberos: protocol

- KDC maakt sleutel
- KDC verdeelt sleutel via ticket (certificaat)
- ticket bevat
  - sessiesleutel
  - principal die sleutel heeft gekregen
  - geldigheidsduur van sleutel
- ticket is versleuteld met unieke geheime sleutel gekend tussen AS en server
- ticket van AS naar server via client

Kerberos: overzicht protocol



Kerberos: dialoog (1x per login)

- Login: loginprogramma → AS **(1)**
  - username
  - id van TGS
  - tijdsaanduiding (controle voor AS)
- AS
  - zoekt username in DB
  - maakt sleutel K_C op basis van opgeslagen wachtwoord
- AS → client: versleuteld met K_C **(2)**
  - sessiesleutel $K_{C,TGS}$
  - identiteit van TGS (laat controle van antwoord toe)
  - tijdsaanduiding + geldigheidsduur van ticket
  - TGT (ticket granting ticket)

Kerberos - X509 - PKI 12

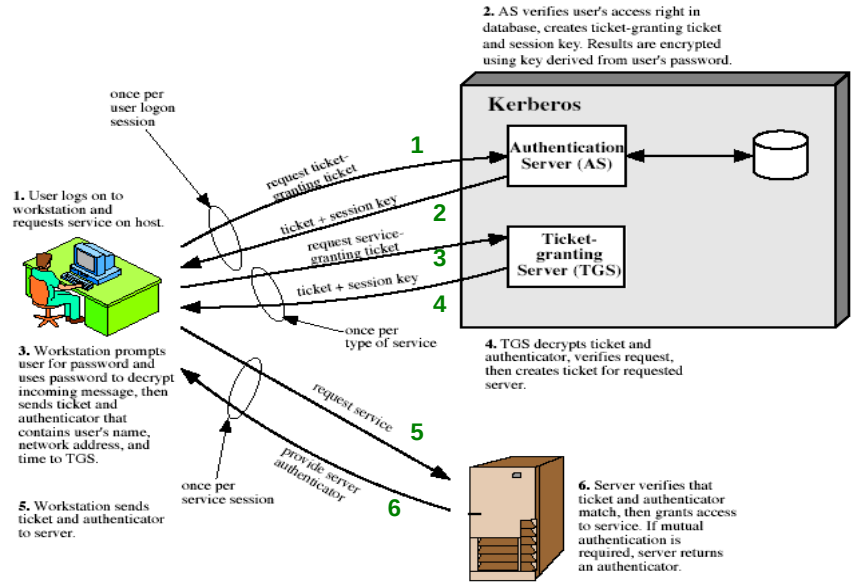
Kerberos: TGT

- betekent dat TGS ticket mag afleveren aan client
- wachtwoord moet dus niet opnieuw worden ingegeven bij aanvraag van ticket voor nieuwe dienst
- TGT is versleuteld met K_{TGS} (geheime sleutel van TGS)
- bevat
  - sessiesleutel $K_{C,TGS}$
  - client id (naam + netwerkadres)
  - identiteit van TGS (controle bij decryptie)
  - tijdsaanduiding en geldigheidsduur
- wordt bewaard door client
- is nodig bij aanvraag van nieuw ticket voor nieuwe dienst

Kerberos: dialoog (logincontrole)

- loginprogramma vraagt wachtwoord aan gebruiker
- maakt sleutel K_C op basis van ingegeven wachtwoord
- ontvangen antwoord in (**2**) wordt gedecrypteerd
- indien geslaagd, succesvolle login

Kerberos: overzicht protocol



Kerberos: dialoog (1x per dienst)

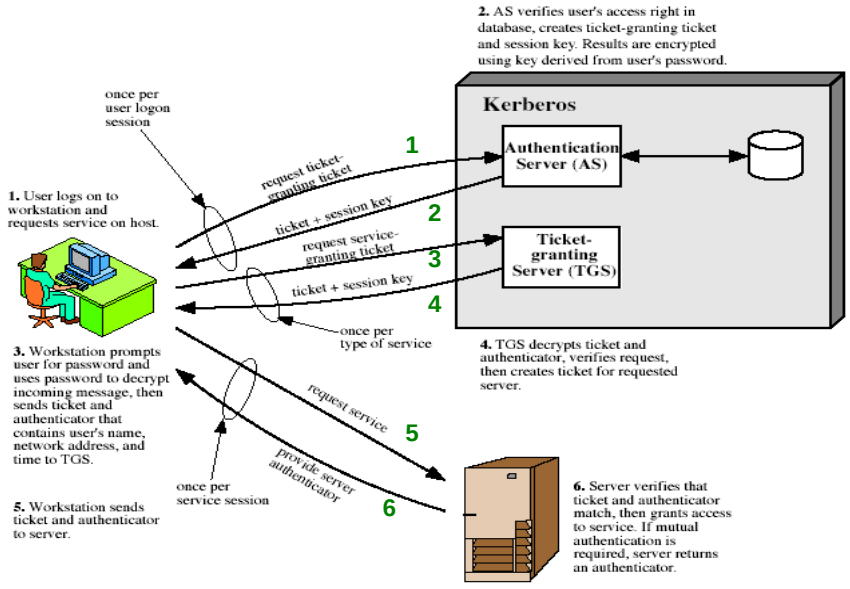
- client vraag ticket aan TGS (**3**)
- bevat
  - id van server of dienst
  - TGT
  - authenticator
- authenticator
  - wordt slecht 1x gebruikt
  - is versleuteld met sessiesleutel $K_{C,TGS}$
  - bevat
    - **client id (naam en netwerkadres)**
    - **tijdsaanduiding**
  - toont recente aanmaak

Kerberos: dialoog (1x per dienst)

- TGS decodeert authenticator
- verifieert echtheid (hoe?)
- TGS → client : versleuteld met $K_{C,TGS}$ **(4)**
  - sessiesleutel $K_{C,V}$ voor verkeer tussen client en server
  - id van server of dienst
  - tijdsaanduiding
  - ticket, versleuteld met geheime sleutel van server K_V
    - **sessiesleutel $K_{C,V}$ voor verkeer tussen client en server**
    - **id van server of dienst**
    - **id van client**
- client bezit herbruikbaar ticket voor server of dienst

Kerberos - X509 - PKI 17

Kerberos: overzicht protocol



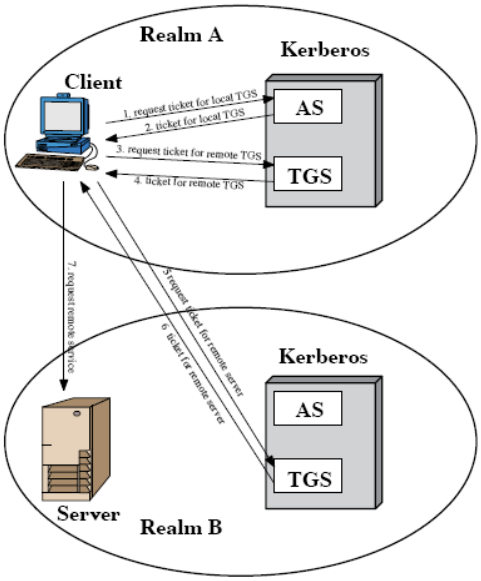
Kerberos: client-server authenticering

- aanvraag van dienst
  client → server **(5)**
  - ticket
  - authenticator, versleuteld met sessiesleutel $K_{C,V}$
    - id van client
    - tijd
- server decodeert ticket en kent sessiesleutel $K_{C,V}$
- server decodeert authenticator
- indien wederzijdse authenticering vereist
  server → client **(6)**
  - tijd+1 versleuteld met sessiesleutel $K_{C,V}$
- sessiesleutel $K_{C,V}$ verder gebruikt bij data-overdracht

Kerberos: meerdere realms

- KDC voorziet niet in registratie van principals uit ander realm
- hoe kan $client_A$ verbinden met $server_B$?
- twee KDC's zijn bij elkaar geregistreerd en delen een sleutel
- stap 4 bevat een ticket voor TGS_B ipv voor server

Kerberos: meerdere realms



21

Kerberos versies

versie 4

- DES
- IP-adres als identificatie
- levensduur in 8 bits stellen n x 5 minuten voor 256 x 5 min = ± 21 uur

versie 5

- aanduiding methode
- andere adresseermethode + aanduiding van het type
- levensduur dmv begin- en eindtijd
- authenticatie kan verder worden doorgestuurd (printserver gebruikt files op remote server)

Kerberos - X509 - PKI 22

X.509 authenticatie

- onderdeel van X.500
  - aanbevelingen van ITU (International Telecom Union) / ISO
  - standaard i.v.m. directory services
  - directory service (LDAP/ActDir) = servers met gedistribueerde gegevensbank met gebruikersinfo
- X.509 = raamwerk: diensten voor (sterke) authenticatie
  - directory bevat certificaten
  - certificaat bevat publieke sleutel van de “gebruiker”
  - certificaat is getekend door certificatieautoriteit
- X.509 definieert ook protocols voor authenticering

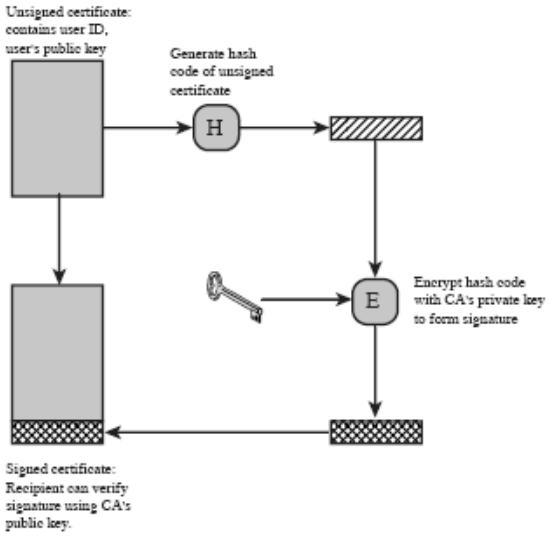
Kerberos - X509 - PKI 23

X.509 authenticering

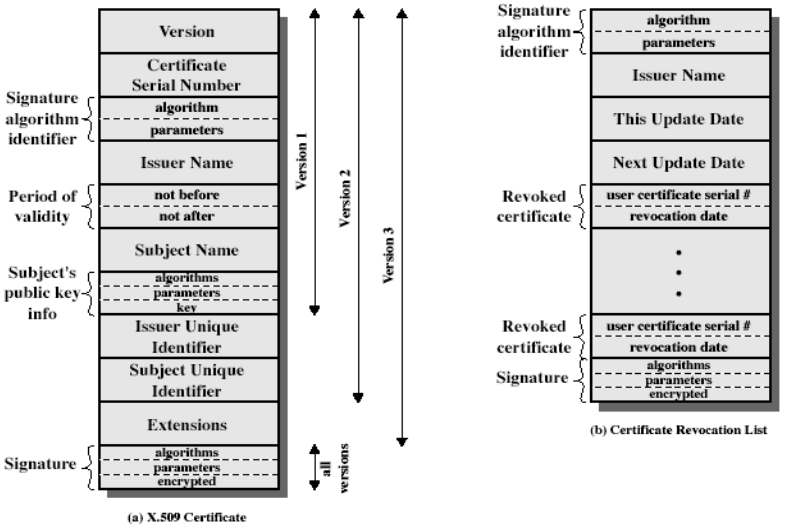
- gebruikt publieke-sleutelencryptie & digitale handtekeningen
- algoritmes zijn niet gestandaardiseerd / RSA aanbevolen
- hash-functie niet gestandaardiseerd
- gebruikt in
  - S/Mime
  - IPSec
  - SSL/TLS
- 1988 - 1993 versie 1 / 1995 versie 3 (2000)
- creëren van certificaat door CA, niet door directory !

Kerberos - X509 - PKI 24

X.509 genereren certificaten



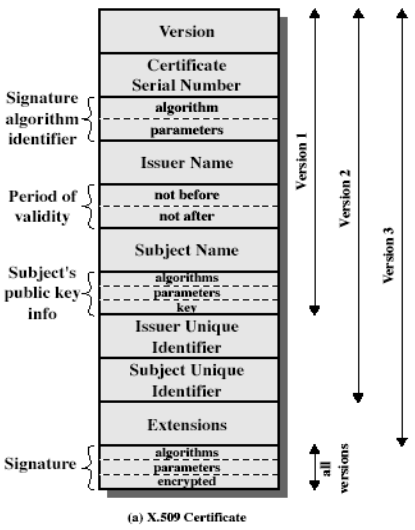
X.509 Certificaten



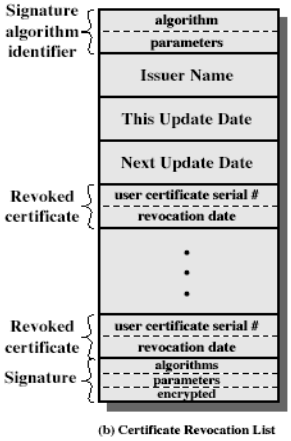
X.509 certificaat

- versienummer
  - 1 bij verstek, 2 als I(ssuer)uid+S(ubject)uid, of 3 indien extensies
- serienummer uniek voor CA, identificeert certificaat
- identificatie van handtekeningalgoritme
  - signature algorithm identifier
  - achteraan herhaald, niet erg nuttig
- naam van uitgever van certificaat (CA)
  - issuer X.500 name (CA)
- geldigheidsperiode
  - period of validity
  - 2 datums: van - tot

X.509 Certificaten



(a) X.509 Certificate



(b) Certificate Revocation List

X.509 certificaat (2)

- onderwerpnaam
  - subject name
  - X.500 naam van eigenaar van publieke sleutel (browser, …)
- publieke-sleutelinformatie van het subject
  - publieke sleutel
  - algoritme waarvoor sleutel kan gebruikt worden + parameters
- vanaf versie 2 (optioneel, weinig gebruikt)
  - issuer unique identifier + subject unique identifier
  - indien X500 namen voor meerdere entiteiten gebruikt zijn
- versie 3: extensies (zie verder)
- handtekening: E_{KRCA}[hash van alle velden]+ id algoritme

Kerberos - X509 - PKI 29

X.509 versie 3 certificaten

- tekortkomingen van versie 1 (alleen identiteit)
  - subject kan geen e-mail, url of andere info bevatten
  - geen informatie over security policy (IPSec)
  - gebruiker moet verschillende sleutels kunnen gebruiken op verschillende momenten (update via CA)
- extra velden in niet-vast formaat, wel generisch
- extensies zijn optioneel
- elke extensie bevat
  - extension type: textstring, numerieke waarde, datum, grafiek,…
  - criticality indicator (true/false)
  - extension value

Kerberos - X509 - PKI 30

Extensies: 4 categorieën

1. informatie over sleutel
   - sleutel id van CA of subject indien meerdere paren bestaan
   - gebruik van sleutel: non-repudiation, tekenen van certificaat of CRL, conventionele encryptie van sleutel of data, DH-key, …
   - geldigheidsperiode voor private sleutel (< dan pub key)
2. informatie over beleid
   - beleid voor certificaat
     - bv. verkoop goederen in bepaalde prijsklasse
     - aangeduid door gestandaardiseerde getallen (ISO)
   - policy-mappings:
     - alleen geldig op cross-certificaten: CA certificeert sleutel van andere CA
     - beleid van de ene CA wordt *gemapt* op beleid van andere

Extensies: 4 categorieën

3. attributen over uitreiker en subject
   - alternatieve namen voor subject:
     e-mailadres, domeinnaam, IP-adres, URI, ...
   - alternatieve namen voor CA
   - extra attributen van subject (postadres, functie, foto, …)
4. restricties van het certificatiepad
   - laat CA vertrouwen van andere CA controleren (kruiscertificatie)
   - basisbeperkingen:
     vb. is subject eindgebruiker of CA (beperking van padlengte)?
   - naambeperkingen:
     vb. tot op welke hoogte vertrouwt CA1 certificaten uitgegeven door CA2? (beperking op basis van naam)
   - beleidsbeperkingen: zoals naambeperking, maar i.v.m. beleid

Aanvragen van een certificaat

- CA is vertrouwde organisatie die link tussen sleutel en identiteit verzekert
- generatie sleutelpaar door applicatie die gecertificeerd moet worden
- private sleutel bewaard in lokale databank
- overdracht van publieke sleutel naar CA
  - niet zonder meer elektronisch
  - identiteit moet gecontroleerd worden
  - fysieke controle moet in proces ingebouwd zijn
- volgende certificaat aanvragen kunnen eerste certificaat gebruiken

Eigenschappen van een certificaat

uitgereikt door CA

- elke gebruiker met toegang tot publieke sleutel van CA kan publieke sleutel van gebruiker verifiëren
- niets of niemand kan certificaat wijzigen
- alleen CA kan certificaat aanpassen
- certificaten kunnen in publieke directory worden geplaatst, vermits ze niet aanpasbaar zijn
- opgelet: certificaten zijn niet versleuteld maar wel gehandtekend

CA hiërarchie

gebruikers behoren tot kleine gemeenschap (school)

- er is 1 CA
- gemeenschappelijk vertrouwen
- alle certificaten in 1directory, voor iedereen toegankelijk
- certificaten kunnen worden doorgestuurd
- veilige gegevensuitwisseling is mogelijk tussen gebruikers

CA hiërarchie (2)

grote gebruikersgemeenschap

- 1 CA is niet praktisch
  - iedereen moet publieke sleutel van CA kennen
  - sleutel moet “veilig” zijn doorgegeven
- voorstel van X.509
  - maak hiërarchie van CA’s
  - verbind alle CA’s in boomstructuur
- notatie
  - CA<<A>> geeft aan
  - A bezit certificaat getekend door CA

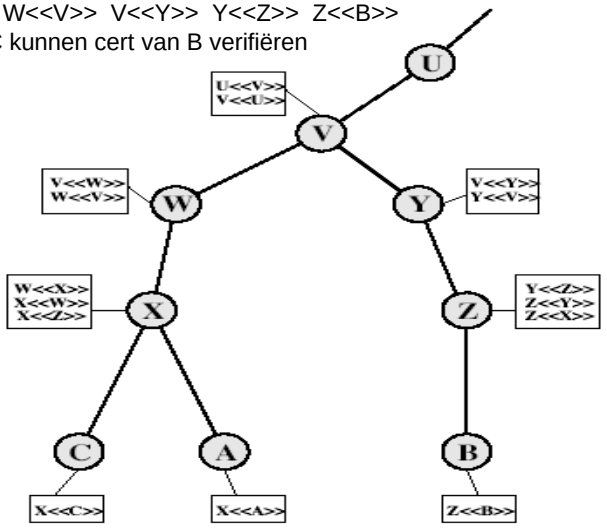
CA hiërarchie (3)

- A bezit certificaat van CA_1, B van CA_2
  - CA_1<<A>> en CA_2<<B>>
  - als A geen vertrouwen heeft in publieke sleutel van CA_2, dan is certificaat van B voor A waardeloos
    A kan sleutel van B afleiden, maar niet verifiëren
- CA_1 en CA_2 moeten mekaars sleutels certificeren
  - CA_1<< CA_2 >>
  - A vertrouwt sleutel van CA_2 want certificaat getekend door CA_1
    - **CA_i<< CA_2 >> CA_2<<B>>**
  - A kan certificaat van B controleren
  - analoog voor B

Kerberos - X509 - PKI 37

CA hiërarchie (4)

X<<W>> W<<V>> V<<Y>> Y<<Z>> Z<<B>>
dus A & C kunnen cert van B verifiëren

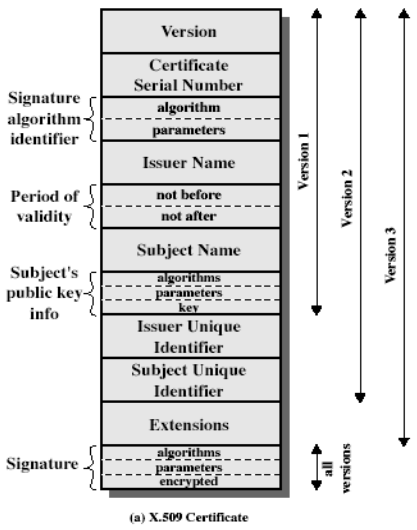


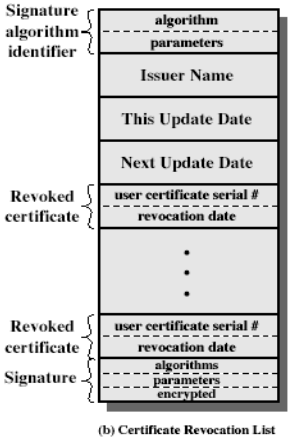
Kerberos - X509 - PKI 38

Revocatie van certificaten

- certificaat heeft beperkte geldigheid (cfr. kredietkaart)
- nieuw certificaat wordt uitgereikt vóór vervaldatum van oud certificaat
- noodzaak om certificaat te herroepen tijdens geldigheidsperiode
  - private sleutel van subject is gecompromitteerd
  - certificaat van CA gecompromitteerd
  - gebruiker niet langer gecertificeerd door CA
- CA onderhoudt lijst van gerevoceerde certificaten uitgereikt door CA
  - Certificate Revocation List of CRL
- gebruikers zouden certificaten moeten nakijken op gerevoceerd zijn

X.509 CRL





Inhoud CRL

- naam van uitgevende CA
- datum van aanmaak van lijst
- voorziene datum van volgende revisie
- ingang voor elk herroepen certificaat:
  - nummer van certificaat
  - revocatiedatum
- handtekening van CA

OCSP

- Online Certificate Status Protocol
- protocol om de revocatiestatus van een X.509 certificaat te bekomen
- RFC 2560
- alternatief voor CRL ivm PKI
- protocol beschrijft boodschappen ← → OCSP-server
- verkregen informatie is meer up-to-date is dan die van CRL
- boodschappen
  - gecodeerd in ASN.1 (Abstract Syntax Notation One)
  - transfer over HTTP
  - vraag+antwoord → server = *OCSP-responder*
- OCSP-server beheerd door CA

OCSP (2)

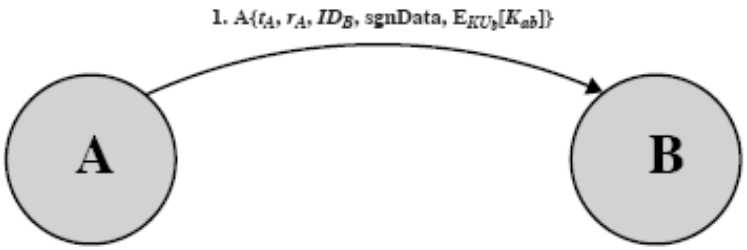
- aanvraag bevat
  - nr van certificaat
  - hash van publieke sleutel
  - nonce N
- antwoord is
  - 'good', 'revoked' of 'unknown‘
  - error-code indien aanvraag niet kan verwerkt worden
  - nonce N
  - getekend door CA, met zelfde sleutel als certificaat
- nonce dient om replay-aanvallen tegen te gaan
  - ‘good’ antwoord later verstuurd naar client na revocatie
- aanvraagformaat ondersteunt meerdere extensies
  - kan aangepast worden aan specifieke vereisten van PKI

Procedures voor authenticatie

X.509 voorziet in 3 alternatieve manieren om te authenticeren

- Authenticatie in 1 stap / richting
- Dubbele authenticatie in 2 stappen
- Authenticatie in 3 stappen
- gebruiken alle 3 publiekesleutelhandtekeningen
- 2 partijen
  A en B, kennen elkaars publieke sleutel

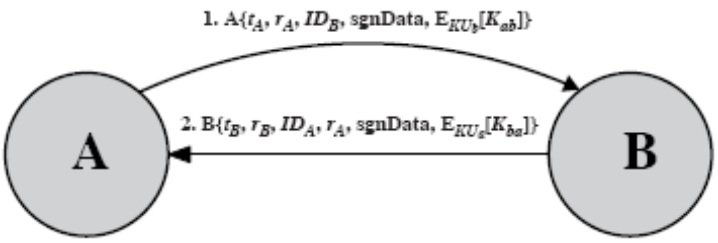
Authenticatie in 1 stap / richting



Authenticatie in 1 stap / richting

- A → B
  - tijdsaanduiding t_A (tegen vertraagde aflevering)
  - nonce r_A (tegen replay)
  - identiteit van B
  - sgnData: hash geëncrypteerd met private sleutel van A
  - eventueel als extra: $E_{KUB}(K_{AB})$
- bewijst:
  - identiteit van A t.o.v. B
  - dat boodschap bestemd is voor B
  - dat boodschap origineel en integer is

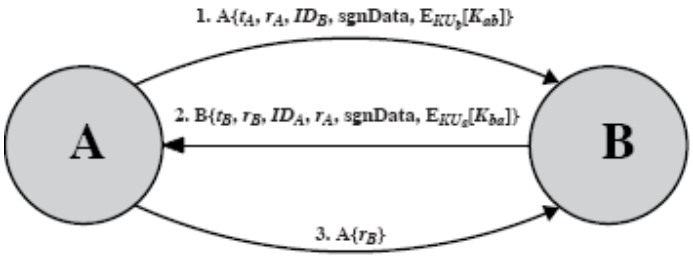
Dubbele authenticatie in 2 stappen



Dubbele authenticatie in 2 stappen

- A → B : zoals hiervoor
- B → A
  - tijdsaanduiding t_B (tegen vertraagde aflevering)
  - nonce r_B (tegen replay)
  - identiteit van A
  - nonce r_A
  - sgnData
  - bewijst:
    - identiteit van B t.o.v. A
    - dat boodschap bestemd is voor A
    - dat boodschap origineel en integer is

Authenticatie in 3 stappen



Authenticatie in 3 stappen

- A → B : zoals hiervoor
- B → A : zoals hiervoor
- A → B
  - rB
  - sgnData
- vermijdt noodzaak van tijdscontrole wegens echoën van nonces