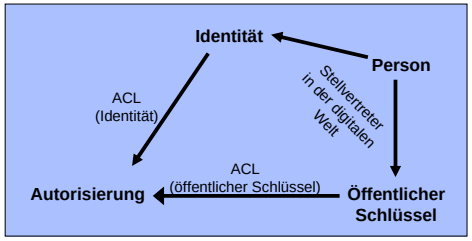
Netzsicherheit – Architekturen und Protokolle
Privilege Management Infrastructure

1. Privilege Management Infrastructure
2. X.509-Attributzertifikate

PMI – Motivation

Autorisierung über Zugangskontrolllisten anhand von

- Identität (via Passwort/Ticket/etc., z.B. pop, imap, smtp-auth)
- Besitz eines privaten Schlüssels (z.B. SSH: authorized_keys)



Problem: Zuordnung von Privilegien zu Personen lokal oder auf Privilegien-Server zentral

Eine PMI ermöglicht eine unabhängige, transportierbare Bindung von Autorisationsdaten

•Eine Autorisierung kann über Zugangskontrolllisten (Access-Control-List - ACL) erfolgen. Zugangskontrolllisten definieren wer auf eine Ressource zugreifen darf. Hier stellt sich die Frage, wie die Zuordnung von Privilegien zu Personen gehandhabt wird. Oft geschieht das auf einer Ressource lokal oder über einen zentralen Privilegien-Server.

•Wie kann man eine unabhängige, transportierbare Bindung von Autorisationsdaten an Identitäten erreichen? Über eine Privilege Mangagement Infrastructure (PMI)!

Access Control Methoden

Im Folgenden betrachtete Access Control Methoden

- Discretionary Access Control
  - individuelle Rechte pro Benutzer
- Mandatory Access Control
  - jede Ressource wird klassifiziert
  - Benutzer bekommen Zugangsrechte zu Klassen
- Role-based Access Control
  - Rechte abhängig von der Rolle des Benutzers
  - Rollen ist eine Menge von Zugriffsrechten zugeordnet
- Hierarchical Role-based Access Control
  - Hierarchische Organisation der Rollen

•Discretionary Access Control :

- •Benutzern werden individuell Rechte pro Ressource vergeben
- •Feingranulare Zugangskontrolle

•Mandatory Access Control

- •Jede Ressource wird klassifiziert
- •Jeder Benutzer wird einer Klasse zugeordnet, für die er Zugangsrechte bekommt (clearance).
  - •z.B. Militär setzt oft folgende Klassen ein: unmarked, unclassified, restricted, confidential, secret, top-secret

•Role-based Access Control

- •Benutzer haben keine individuellen Rechte, sondern Rechte abhängig von ihrer Rolle, z.B. Position in der Firma
- •Rollen wiederum werden eine Menge von Zugriffsrechten zugeordnet

•Hierarchical Role-based Access Control

- •Rollen können hierarchisch organisiert werden, d.h. höhere Rollen bauen auf niedrigeren Rollen auf
- •Höhere Rollen erben eventuell die Zugriffsrechte von niederen Rollen

Beispiel

- Discretionary Access Control

Datei A

Datei B

Datei C

Alice:

Datei A: Lesen
Datei B: Lesen, Schreiben

Bob:

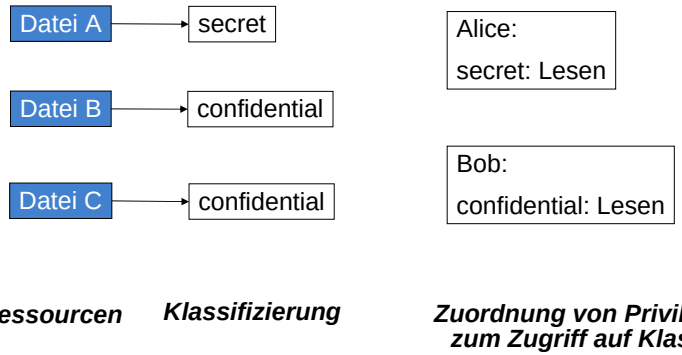
Datei B: Lesen
Datei C: Lesen

Ressourcen ***Zuordnung von Privilegien***

Achtung: In den folgenden Folien wird die zu Grunde liegende Idee der verschiedenen Access Control Mechanismen noch einmal allgemein beschrieben. Hier wird noch kein Hinweis auf die konkrete Realisierung (z.B. über X.509-Zertifikate) gegeben.

Beispiel

- Mandatory Access Control

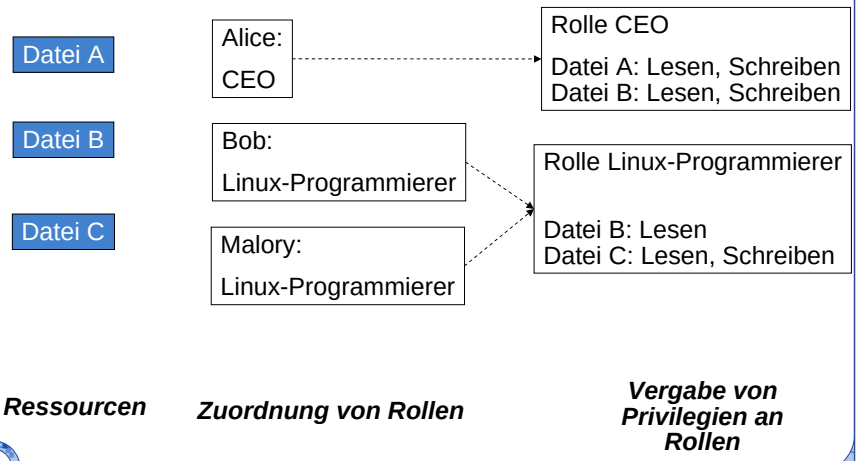


Im Zusammenhang mit Mandatory Access Control wird oft die Security Policy „read down and write up“ verwendet: Die Privilegien werden so vergeben, dass es einem Benutzer, dem eine Klasse zugeordnet wurde, möglich ist, auch Ressourcen mit einer niedrigeren Klasse zu lesen. Er darf aber nur Ressourcen erstellen oder ändern, die seine Klasse oder eine höhere Haben.

Frage: Wozu dient diese Security Policy?

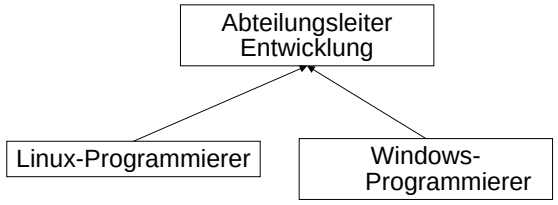
Beispiel

- Role-based Access Control



Beispiel

- Hierarchical Role-based Access Control



- Abteilungsleiter erhält auch die Privilegien von Linux-Programmierer und Windows-Programmierer

Autorisierung

- Authentifikation → realisiert über ID-Zertifikate
- Wie kann Autorisierung realisiert werden?
  - welcher Benutzer hat in Bezug auf eine Ressource welche Privilegien?
  - wer darf Privilegien vergeben?
  - wer darf Privilegien weitergeben?

•Authentifikation: über ID-Zertifikaten und der Public Key Infrastructure zu deren Verwaltung gelöst

Attributzertifikate

Nachweis der Autorisierung über Attributzertifikate

- attestieren Identität bestimmtes Privileg (=Attribut)
- zeitlich einschränkbar
- basieren auf PKI und deren ID-Zertifikaten
- können widerrufen werden
  (Attribute Certificate Revocation List)

Analog zur PKI ist eine Infrastruktur zum Management dieser Zertifikate notwendig

Privilege Management Infrastructure

•Zur Erinnerung: Attributzertifikate binden Attribute (z.B. Privilegien) an eine Identität.

•Vorsicht: Attributzertifikate und Autorisierungszertifikate sind nicht das Gleiche!

Privilege Management Infrastructure

Aufbau einer PMI ähnlich Aufbau einer PKI

- *CA der PMI*: *Attribute Authority* (AA)
  - vergibt Zugriffsrechte
  - zertifiziert diese Rechte in Form von Attributzertifikaten
- *Root CA der PMI*: *Source of Authority* (SOA)
  - Verifizierung eines Privilegs beginnt bei der SOA
  - oberste AA für dieses Privileg
  - Attributzertifikat der SOA
    - selbstzertifiziert
    - signiert mit dem zum ID-Zertifikat der SOA gehörenden privaten Schlüssel

•Eine Privilege Management Infrastructure (PMI) ist eine Infrastruktur zum Management von Zugriffsrechten basierend auf Attributzertifikaten.

•Eine CA (einer PKI) kann auch AA (einer PMI) sein, meist sind diese Funktionalitäten allerdings getrennt. Mehrere AAs (einer PMI) bauen meist auf einer einzigen CA (einer PKI) auf.

Gegenüberstellung Begriffe PKI/PMI

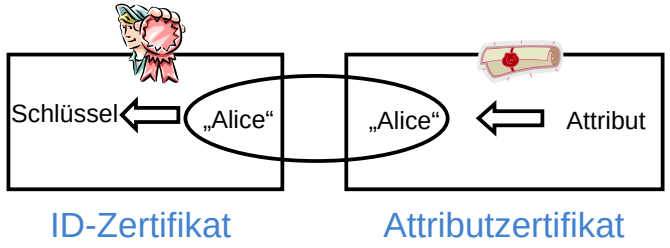
Konzept	PKI	PMI
Zertifikatsbezeichnung	Public Key- bzw. ID-Zertifikat	Attributzertifikat
Zertifizierender	Certificate Authority (CA)	Attribute Authority (AA)
Zertifizierter	Subject	Holder
Zertifizierter Inhalt	ID an Public Key	Attributwerte an ID
Widerruf	CRLs: EPRLs/CARLs	ACRLs: EARLs/AARLs
Vertrauensanker	Root Certificate Authority (Root-CA)	Source of Authority (SOA)

•EARL=End-Entity Attribute Certificate Revocation List => enthält Widerrufsinformationen über Endbenutzer-Attributzertifikate.

•AARL=Attribute Authority Certificate Revocation List => Enthätlt Widerrufsinformationen über AA-Zertifikate

•Zertifizierter Inhalt: Durch Extensions können weitere „Werte“ an den Schlüssel gebunden: Alternativer Name, Rollen, …

Attribut-Zertifikat und ID-Zertifikat

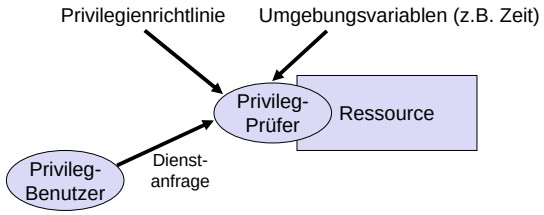


•Das Zusammenspiel von Attributzertifikaten mit ID-Zertifikaten erfolgt also über die Identität, im Beispiel der Name „Alice“

PMI-Grundmodell

Allgemeines Modell

- Privileg-Prüfer (*privilege verifier*)
- Privileg-Benutzer (*privilege asserter*)
- Ressource, auf die zugegriffen wird
- Privilegien-Richtlinie (*privilege policy*)
- Umgebungsvariablen (z.B. aktuelle Zeit)



•Der Privileg-Benutzer verfügt über ein Attributzertifikat für das Privileg. Er stößt den Zugriff auf eine Ressource an und damit die Zugriffsprüfung durch den Privilegien-Prüfer

•Die Zugriffsprüfung wird durch den Privileg-Prüfer vorgenommen. Der Privileg-Prüfer trifft im Rahmen des Prüfungsprozesses eine Ja/Nein-Entscheidung ob dem Privileg-Benutzer der Zugriff gewährt wird.

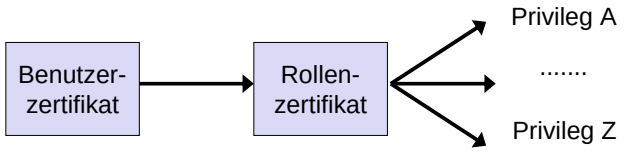
•Die Privilegien-Richtlinie gibt genau an, welche Menge von Privilegien notwendig ist, damit der Privileg-Prüfer Zugriff zur Ressource gibt. Unter Umständen sind zum Zugriff also mehrere Privilegien notwendig.

•Weitere Umgebungsvariablen wie z.B. die Zeit spielen bei der Prüfung eine Rolle, da Privilegien z.B. zeitlich eingeschränkt sein können.

PMI-Grundmodell

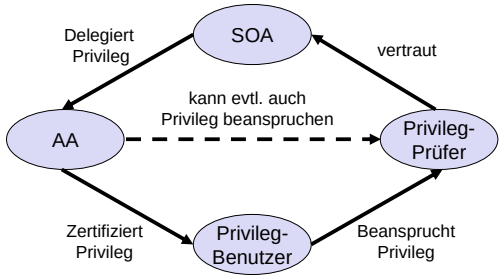
Rollen

- Rolle steht stellvertretend für Menge von Privilegien
- Privilegien der Rolle werden ebenfalls in einem Attributzertifikat spezifiziert, können somit jeder Zeit geändert werden



PMI-Vertrauensmodell

- „Single-CA“ mit Delegierung
  - SOA vergibt die Privilegien an AAs
  - AAs können Privilegien weiter delegieren
  - nur eigene Privilegien oder Untermenge delegierbar
  - ermöglicht natürliche Verteilung der Privileg-Zuweisung
  - zur Verifizierung muss Pfad von AAs aufgebaut werden



•Vertrauensmodelle sind bei heute verfügbaren PMIs meist nicht sehr ausgeprägt und gehorchen üblicherweise dem analogen Konzept von „Singe-CA“ mit Deligierung.

•Ebenso wie bei einer PKI muss bei einer PMI zur Überprüfung eines Attributzertifikats ein Pfad zwischen der ausstellenden AA und der SOA aufgebaut werden.

Netzsicherheit – Architekturen und Protokolle
Privilege Management Infrastructure

1. Privilege Management Infrastructure
2. X.509-Attributzertifikate

X.509-PMI

- Seit der letzten Edition spezifiziert X.509 ein detailliertes Framework zur Autorisierung authentifizierbarer Schlüsselbesitzer
- X.509 bietet zwei Wege zur Autorisierung an
  - Privilegien in ID-Zertifikaten
  - Privilegien in Attribut-Zertifikaten

Diskussion

- Welche Vor- und Nachteile haben Privilegien in ID-Zertifikaten?
- Welche Vor- und Nachteile haben Privilegien in Attribut-Zertifikaten?

Privilegien in ID-Zertifikaten

- X.509 Erweiterung subjectDirectoryAttributes enthält Privilegien
- CA muss auch AA für die Ressource sein
  - in Praxis eher nicht der Fall
- Dauer der Privilegien- und ID-Zertifizierung muss gleich sein
  - Widerruf einzelner Privilegien nicht möglich
  - Zertifikat nur als Ganzes widerrufbar
- Nur gesamte Menge an Privilegien delegierbar (keine Untermenge)

Privilegien in Attributzertifikaten

- Attestieren einer Identität bestimmte Privilegien
  - Privilegien können getrennt von ID-Zertifizierung vergeben werden
    - CA muss nicht gleichzeitig AA sein
  - mehrere unabhängige Privilegien in getrennten Zertifikaten zuweisbar
    - jedes Zertifikat kann einzeln widerrufen werden
  - Gültigkeitsdauer der Privilegien beliebig
    - insbesondere auch kürzer als zugeh. ID-Zertifikat möglich
  - Delegation einer Untermenge von Privilegien möglich

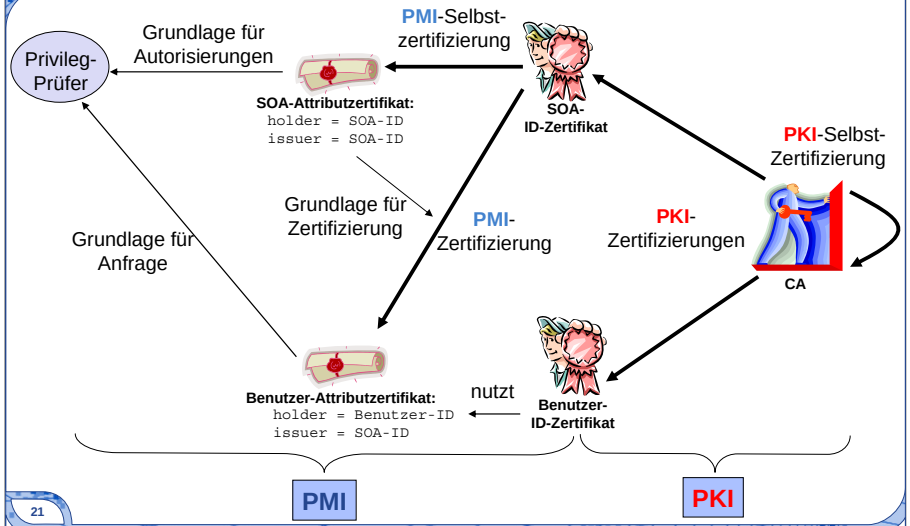
•Attributzertifikate bieten also eine größere Flexibilität im Vergleich zu ID-Zertifikaten

Aufbau eines Attribut-Zertifikates

Ein Attributzertifikat besteht aus einer signierten Ausgabe folgender Daten

Feld	Beschreibung
`version`	Versionsnummer des Formates
`holder`	Verweis auf ID-Zertifikat des Besitzers • ID der CA+Seriennummer des ID-Zertifikats
`issuer`	Verweis auf ID-Zertifikat der AA
`signature`	für die Signatur genutzter Algorithmus
`serialNumber`	Seriennummer
`attCertValidityPeriod`	Gültigkeitsdauer • `notBeforeTime` • `notAfterTime`
`attributes`	Zertifizierte Attribute
`issuerUniqueID`	ID der austellenden AA
`extensions`	Erweiterungen

PKI/PMI: Big Picture (ohne Delegation)



•Die CA verfügt über ein selbstzertifiziertes ID-Zertifikat, während die SOA über ein selbstzertifiziertes Attributzertifikat, das SOA-Attributzertifikat verfügt. Die PKI stellt dem Benutzer und der SOA jeweils ID-Zertifikate aus. Die SOA stellt dem Benutzer im Rahmen der PMI das Benutzer-Attributzertifikat aus.

•Der Privilegien-Prüfer muss über das SOA-Attributzertifikat als Grundlage der Privilegien-Prüfung verfügen. Weiterhin muss der Privilegien-Prüfer über eine Möglichkeit verfügen, ID-Zertifikate zu verifizieren (z.B. indem er über das ID-Zertifikat der CA verfügt)

Basiserweiterungen

Verwendung des Erweiterungsmechanismus um komplexere Szenarien abzubilden

- Basiserweiterungen
  - **`timeSpecification`**
    - zeitliche Einschränkung der Nutzung (nicht Delegierung!) eines Privilegs
    - z.B. während Bürozeiten, Mo - Fr von 08:00 – 18:00 Uhr
  - **`acceptablePrivilegePolicies`**
    - spezifiziert akzeptable Privilegienrichtlinen
    - ist vom Dienstgeber zu prüfen
    - Flag critical ist für diese Erweiterung immer gesetzt

•Hinweis: Während attCertValidityPeriod die Zeit einschränkt, in der ein X.509-Attributzertifikat gültig ist, schränkt timeSpecification die Zeit ein, in der ein Privileg genutzt werden kann!

Widerruferweiterungen

- Widerruferweiterungen
  - **`CRLdistributionPoint`**
    - gibt an, wo die Attribute Certificate Revocation List zu finden ist (wie bei ID-Zertifikaten)
  - **`noRevAvail`**
    - gibt an, dass dieses Zertifikat nicht widerrufen werden kann
      - oft bei kurzlebigen Zertifikaten

•Mit CRLdistributionPoint ist es insbesondere möglich, dass verschiedene Attributzertifikate auch verschiedene ACRLs benutzen können, so dass diese Listen nicht zu lange werden.

SOA-Erweiterungen

Optionale Autorisierung eines ID-Zertifikates, SOA sein zu dürfen, über folgende Erweiterung

- **`sOAIdentifier`**
  - Identifiziert den Inhaber eines ID-Zertifikates als SOA
  - ermächtigt Inhaber
    - Attribute zu definieren, Privilegien zuweisen
    - Zertifikate zu erstellen, die diese beschreiben (Attributbeschreibungszertifikat)
    - Privilegien anderen Nutzern zuzuteilen

•Attributbeschreibungszertifikat= attribute descriptor certificate

Attributbeschreibungszertifikat

Beschreibung der Bestandteile eines Attributes über ein *Attributbeschreibungszertifikat* das die Erweiterung **`attributeDescriptor`** enthält

- selbstsigniert
- beschreibt ein Attribut
  - ID, Name
  - Syntax, Beschreibung
  - Definition der Enthaltensein-Relation (*attribute domination*)

•Die Enthaltensein-Relation eines Attributes ist insbesondere wichtig um Untermengen von Privilegien festzulegen. Beispiel: Die SOA delegiert nur einen Teil der Privilegien an eine AA.

Rollen-Erweiterung

Ermöglicht die Verwendung von Rollen

- Attributzertifikat des Benutzers enthält bei Zuweisung einer Rolle folgende Erweiterung
  - **`roleSpecCertIdentifier`**
    - Name der Rolle
    - Aussteller des Rollen-Zertifikats
    - Seriennummer des Rollen-Zertifikats
    - Ort wo das Zertifikat zu finden ist
- Rollenzertifikat an sich
  - ist gekennzeichnet durch das Attribut **`role`**
    - **`roleName`** gibt den Namen der Rolle an
    - **`roleAuthority`** nennt ID der Instanz, die Rolle definiert hat
  - enthält die tatsächlichen Attributswerte

•Rolle = Alternative zur direkten Privilegienzuweisung: Einer Rolle werden Privilegien zugewiesen. Ein Benutzer kann zu einer bestimmten Zeit eine Rolle ausfüllen.

•Frage: Unterschied roleAuthority und issuer?

Delegierungserweiterungen

Erweiterungen zur Kontrolle der Delegation

- **`basicAttConstraints`**
  - gibt an, ob Zertifikatsinhaber das Privileg weiterdelegieren darf, d.h. AA ist
  - maximale Zertifikat-Pfadlänge spezifizierbar
- **`delegatedNameConstraints`**
  - schränkt den Namensraum der Zertifikatsbesitzer ein, denen Zertifikate ausgestellt werden dürfen
  - **`permittedSubtrees`**, **`excludedSubtrees`**

•Wie bei ID-Zertifikaten gibt es auch bei Attributzertifikaten Erweiterungen, die die Delegierung kontrollieren

•AA-ID-Zertifikat: Privilegien in einem ID-Zertifikat

•AA-Attributzertifikat: Privilegien in einem gesonderten Attributzertifikat

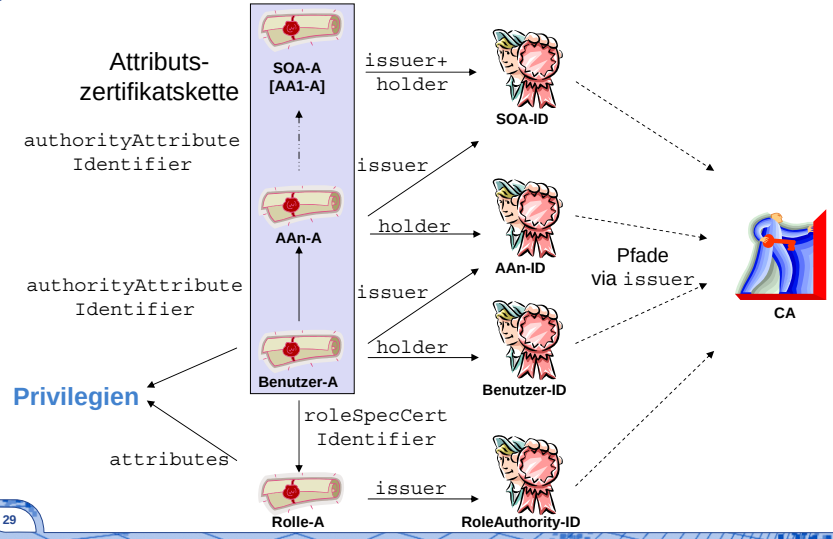
Delegierungserweiterungen

Erweiterungen zur Kontrolle der Delegation

- **`acceptableCertPolicies`**
  - Einschränkung der Zertifikatbesitzer, die Privilegien bekommen
    - nur Besitzer gewisser ID-Zertifikate werden akzeptiert
    - Anhand von Zertifizierungsrichtlinien der CA
- **`authorityAttributeIdentifier`**
  - verweist auf das Attribut-Zertifikat, das dem Issuer den Status als AA verleiht
  - wird benutzt, um Zertifikatskette zu erstellen

•acceptableCertPolicies bezieht sich auf die zugehörigen ID-Zertifikate und nicht auf Attributzertifikate, also auf eine PKI und nicht auf die PMI!

PKI/PMI: Big Picture (im Detail)



•Die Zertifikatskette wird von der ausstellenden AA aus über die Erweiterung „authorityAttributeIdentifier“ aufgebaut, da dieses jeweils auf das nächste Attributzertifikat Richtung SOA verweist.

Validierung von Privilegien

1. Aufbau der Attributszertifikatskette (Benutzer bis SOA)
2. Verifizieren der Signaturen der Attributszertifikatskette
3. Validieren der ID-Zertifikate (siehe PKI), die in der Kette referenziert werden
4. Prüfen der Gültigkeit der Attributs- und ID-Zertifikate (Dauer, Zeitpunkt, Richtlinien, Einschränkungen, Widerruf, etc.)
5. Prüfen, ob alle Attributzertifikate zwischen SOA und Nutzer
   1. autorisierte AAs sind
   2. gültig sind in Hinsicht auf Pfad- und Namenseinschränkungen
   3. durch ID-Zertifikate authentifiziert sind, die unter einer gegebenen Richtlinie gültig sind
   4. die Dominierungsregel korrekt angewandt haben (nicht mehr Rechte weitergegeben wurden, als man selbst besitzt)

Autorisierungsmodelle mit X.509

Realisierung der Modelle mit X.509

- Discretionary Access Control
  - individuelle Privilegien in Attributzertifikaten der Benutzer
- Mandatory Access Control
  - Benutzer werden Klassen und erlaubte Aktionen in Attributzertifikat zugewiesen
- Role-based Access Control
  - mittels `roleSpecCertIdentifier` Verweis auf Rollen-Zertifikat
  - Rollen-Zertifikat ist Attributzertifikat mit Attribut `role`
- Hierarchical Role-based Access Control
  - innerhalb von Rollen-Zertifikat Verweis auf weitere Rollen möglich

Bewertung von X.509-PMI

- Vorteile der X.509-PMI
  - ☺ Aufgabentrennung möglich
    - PKI für Authentifizierung zuständig
    - PMI mit AAs für Autorisierung zuständig

    → sehr flexible Aufgaben- und Rechteverteilung möglich
  - ☺ Abbildung auf Unternehmensstrukturen einfach durch Delegation

- Nachteile der X.509-PMI
  - ☹ Autorisierung mit Attributzertifikaten geschieht in zwei Schritten
    - öffentlicher Schlüssel – Identität
    - Identität – Privileg

    und ist somit an zwei Stellen angreifbar
  - ☹ Validierung aufwendig
  - ☹ Autorisierung basiert auf Namen, die jedoch selten relevant sind (Alternative: Autorisierung basierend auf öffentlichem Schlüssel)

Literatur

- ITU-T Recommendation X.509 (03/00) http://www.itu.int/rec/T-REC-X.509-200003-I/en
- David Chadwick, „The X.509 Privilege Management Infrastructure“, https://www.cs.kent.ac.uk/pubs/2004/2278/content.pdf
- PKI, PMI und X.509 Zusammenfassung http://www.cryptoshop.com/de/knowledgebase/pki/index.php