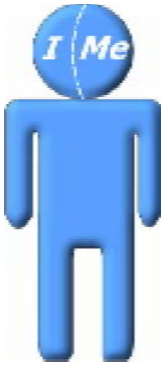
Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

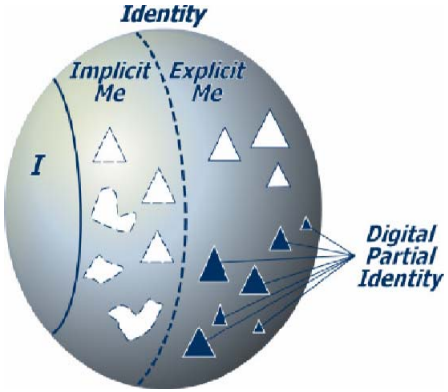
Identitätsmanagement

„Who is the Matthias on your site?“

Die Identität

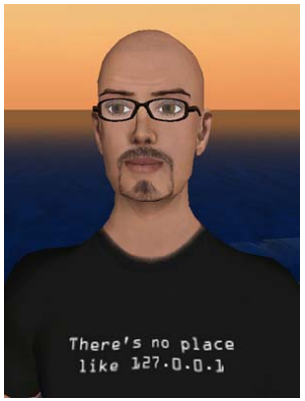


physische Identität

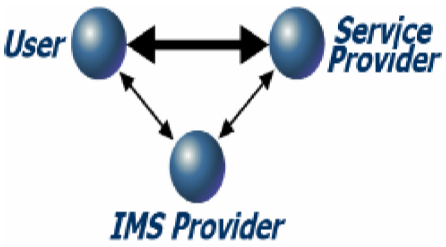


digitale Identität

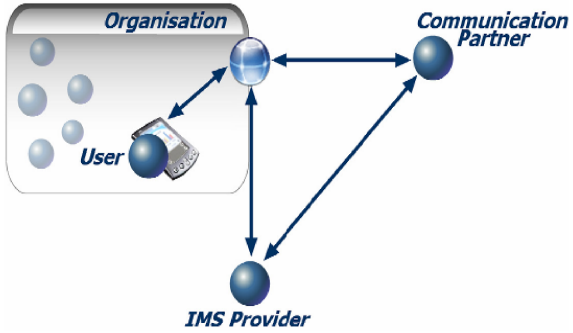
virtuelle Identität



Aber was ist **Identität**?

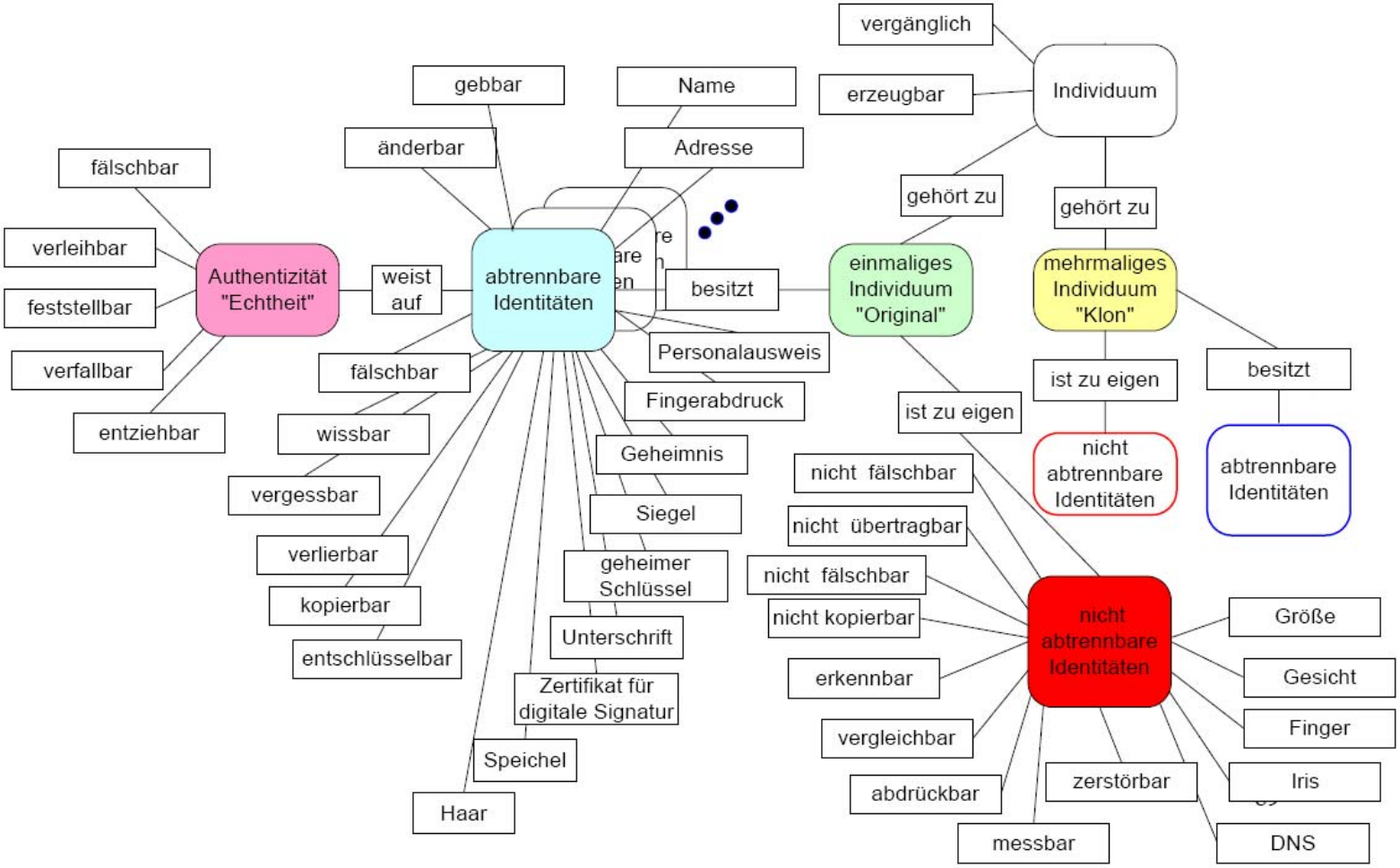


individuelle Identität



Organisations-Identität

Identität


vergänglich
erzeugbar
Individuum
gebbar
Name
änderbar
Adresse
fälschbar
gehört zu
gehört zu
verleihbar
Authentizität "Echtheit"
weist auf
abtrennbare Identitäten
besitzt
einmaliges Individuum "Original"
mehrmaliges Individuum "Klon"
feststellbar
verfallbar
fälschbar
Personalausweis
ist zu eigen
besitzt
entziehbar
wissbar
Fingerabdruck
ist zu eigen
Geheimnis
nicht abtrennbare Identitäten
abtrennbare Identitäten
nicht fälschbar
vergessbar
Siegel
nicht übertragbar
verlierbar
geheimer Schlüssel
nicht fälschbar
kopierbar
nicht kopierbar
nicht abtrennbare Identitäten
Größe
Unterschrift
entschlüsselbar
erkennbar
Gesicht
Zertifikat für digitale Signatur
vergleichbar
Finger
Speichel
abdrückbar
zerstörbar
Iris
Haar
messbar
DNS

Identität

Identität:

völlige Übereinstimmung der überpüfbaren Eigenschaften eines Individuums(*) mit dessen unverwechselbaren Eigenschaften (Zo- Anm.: unverwechselbare Eigenschaften können nicht gewechselt werden (?))

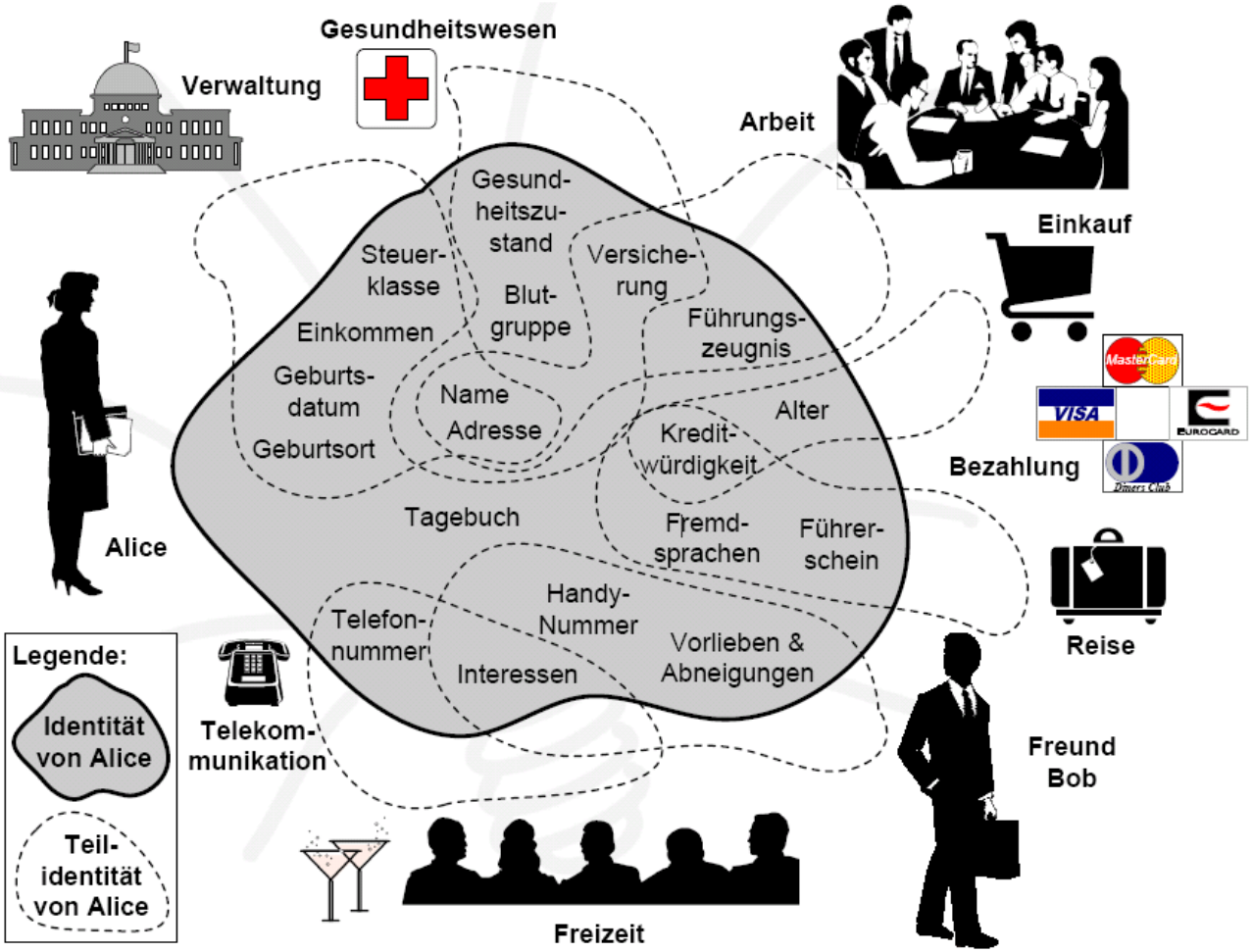
Identität:

die völlige Übereinstimmung einer Person oder Sache mit dem, was sie ist oder als was sie bezeichnet wird

Identifizieren [nach Wendt]

- Benennen = I. beim Namen nennen
- Zeigen = I. auffindbar machen
- Umschreiben = I.s Identitäten(t/u) angeben

Identität


Gesundheitswesen
Verwaltung
Arbeit
Einkauf
Gesund-
heitszu-
stand
Steuer-
klasse
Versiche-
rung
Blut-
gruppe
Führungs-
zeugnis
Einkommen
Geburts-
datum
Name
Adresse
Alter
Geburtsort
Kredit-
würdigkeit
Bezahlung
Tagebuch
Fremd-
sprachen
Führer-
schein
Alice
Handy-
Nummer
Telefon-
nummer
Vorlieben &
Abneigungen
Interessen
Reise
Legende:
Identität
von Alice
Teil-
identität
von Alice
Telekom-
munikation
Freund
Bob
Freizeit

Identität

	1 Teilidentität	>1 Teilidentität		keine Identität
		mit Nutzerkontrolle	ohne Nutzerkontrolle	
ohne IT	Personalausweis	Kommunikation zwischen Personen	Gerüchte	oberflächliche Transaktion
mit IT	elektronische Gesundheitskarte	??	Profiling	Anonymisierer

Identitätsmanagement

Identitätsmanagement ist die Verwaltung von Identitäten und/oder von Identitätsdaten.

Als **Identitätsmanagement** (IdM) wird der zielgerichtete und bewusste Umgang mit Identität, Anonymität und Pseudonymität bezeichnet. (Wikipedia, 8.11.2007)

Der Zweck des **Identity and Access Management (IAM)** ist die Vielzahl der Kennungen und personenbezogenen Informationen welche die Anwender für den Zugriff auf Applikationen, Ressourcen und IT-Systeme benötigen, zu *reduzieren* und nach Möglichkeit in einer einzigen digitalen Identität **zusammenzufassen**. (www.iam-wiki.org, 8.11.2007)

Identitätsmanagementsystem

	Account Management *zugewiesene Identität*	durch die Organisation
	Verwaltung eigener (Teil-)Identitäten *gewählte Identität*	durch den Nutzer (mit Hilfe von Dienstleistern)
	Profiling *abgeleitete Identität*	durch eine Organisation

Authentifizierung

Identifikation: Feststellen einer Identität (Verb: Identifizieren)

Authentifikation: Feststellung der Echtheit (Verb: Authentifizieren)

sich identifizieren: nachweisen, dass man der- oder diejenige ist, die er oder sie vorgibt, zu sein (syn. oft: **sich authentifizieren)**

(nach Zorn)

Authentifizierung (v. griech. *authentikos* für „Urheber“, „Anführer“) ist der Vorgang der Überprüfung (Verifikation) einer behaupteten Authentizität, beispielsweise einer Person oder eines Objekts, z.B. eines Computersystems. (Wikipedia, 8.11.2007)

Autorisierung

Autorisierung ist im weitesten Sinne eine Zustimmung, spezieller, die Einräumung von Rechten gegenüber Anderen, ggf. zur Nutzung gegenüber Dritten. In der Informationstechnologie bezeichnet sie die Zuweisung und Überprüfung von Zugriffsrechten auf Daten und Diensten an Systemnutzer. (Wikipedia, 8.11.2007)

Agenda

1. Die grundlegenden Fragen
    1. Identität
    2. Identitätsmanagement(-systeme)
    3. Authentifizierung & Autorisierung
2. Die Vergangenheit
    1. klassische Authentifikation
    2. Access Control Lists
3. Die Gegenwart
    1. Verzeichnisdienste
    2. verteile Authentifizierung
    3. Role Based Access Control
4. Die Wünsche für die Zukunft
    1. Trusted Source of Authority
    2. Single Sign-On
    3. Privacy
5. Die Hoffnungsträger
    1. federated Identity
        1. Shibboleth
    2. Identity 2.0
        1. OpenID
        2. Information Cards

Agenda

1. Die grundlegenden Fragen
    1. Identität
    2. Identitätsmanagement(-systeme)
    3. Authentifizierung & Autorisierung
2. Die Vergangenheit
    1. klassische Authentifikation
    2. Access Control Lists
3. Die Gegenwart
    1. Verzeichnisdienste
    2. verteile Authentifizierung
    3. Role Based Access Control
4. Die Wünsche für die Zukunft
    1. Trusted Source of Authority
    2. Single Sign-On
    3. Privacy
5. Die Hoffnungsträger
    1. federated Identity
        1. Shibboleth
    2. Identity 2.0
        1. OpenID
        2. Infromation Cards

klassische Authentifizierung

Biometrie

HTTP-Digest-Authentication

PIN/TAN/RSA-Token

X.509-Zertifikate

HTTP-Basic-Authentication

HTTP-Basic-Authentifizierung

- einfachste Methode für die Übermittlung von Credentials (hier: Benutzername + Passwort)
- bereits in HTTP 1.0 enthalten(RFCs 1945, 2616, 2617)
- basiert auf Vertraulichkeit der Übertragung ← Credentials werden nur Base64 enkodiert

```
GET /private/index.html HTTP/1.0
Host: localhost
```

```
HTTP/1.0 401 UNAUTHORIZED
...
WWW-Authenticate: Basic realm="SokEvo" Content-Type: text/html
...
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=ISO-8859-1">
...
```

```
GET /private/index.html HTTP/1.0
Host: localhost
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

```
HTTP/1.0 200 OK
...
```

HTTP-Digest-Authentifizierung

- Erweiterung des HTTP-Protokolls (RFCs 2069, 2671)
- designierter Nachfolger der Basic-Authentifizierung
- einfache Anwendung der MD5-Kryptographie → keine Übermittlung oder Speicherung von Klartext-Passwörtern notwendig
- Verwendung von nonce-Werten → Verhinderung von Replay- und Chosen-Plaintext-Angriffen
- allerdings: viele Sicherheitsfeatures nur optional, inkompatibel mit den meisten Datenquellen

```
HA1 = MD5(A1) = MD5(username : realm : password)
HA2 = MD5(A2) = MD5(method : digestURI)
response = MD5(HA1 : nonce : nonceCount :clientNonce : qop : HA2)
```

HTTP-Digest-Authentifizierung


```
GET /dir/index.html HTTP/1.0
Host: localhost
```

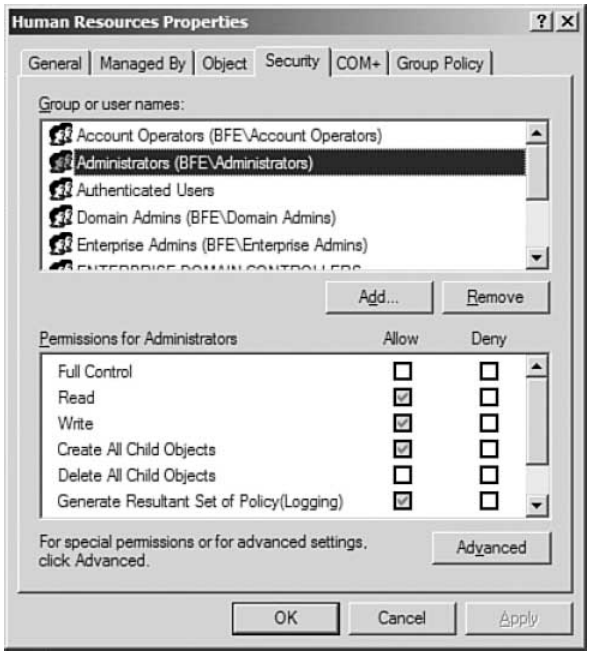
```
HTTP/1.0 401 Unauthorised
Server: SokEvo/0.9
Date: Sun, 10 Apr 2005 20:26:47 GMT
WWW-Authenticate: Digest
            realm=testrealm@host.com,  qop="auth,auth-int",
            nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
            opaque="5ccc069c403ebaf9f0171e9517f40e41"
Content-Type: text/html
Content-Length: 311
...
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=ISO-8859-1">
...
```

```
GET /dir/index.html HTTP/1.0
Host: localhost Authorization: Digest
             username="Mufasa", realm="testrealm@host.com",
             nonce="dcd98b7102dd2f0e8b11d0f600bfb0c093",
             uri="/dir/index.html", qop=auth, nc=00000001,
             cnonce="0a4f113b",
             response="6629fae49393a05397450978507c4ef1",
             opaque="5ccc069c403ebaf9f0171e9517f40e41"
```

```
HTTP/1.0 200 OK
...
```

Access Control Lists

In computer security, an **access control list** (**ACL**) is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. In a typical ACL, each entry in the list specifies a subject and an operation: for example, the entry (Alice, delete) on the ACL for file XYZ gives Alice permission to delete file XYZ. (Wikipedia, 8.11.2007)



Capabilities

A **capability** is defined to be a protected object reference which, by virtue of its possession by a user process, grants that process the capability (hence the name) to interact with an object in certain ways. Those ways might include reading data associated with an object, modifying the object, executing the data in the object as a process, and other conceivable access rights. (Wikipedia, 8.11.2007)

Agenda

1. Die grundlegenden Fragen
    1. Identität
    2. Identitätsmanagement(-systeme)
    3. Authentifizierung & Autorisierung
2. Die Vergangenheit
    1. klassische Authentifikation
    2. Access Control Lists
3. Die Gegenwart
    1. Verzeichnisdienste
    2. verteile Authentifizierung
    3. Role Based Access Control
4. Die Wünsche für die Zukunft
    1. Trusted Source of Authority
    2. Single Sign-On
    3. Privacy
5. Die Hoffnungsträger
    1. federated Identity
        1. Shibboleth
    2. Identity 2.0
        1. OpenID
        2. Infromation Cards

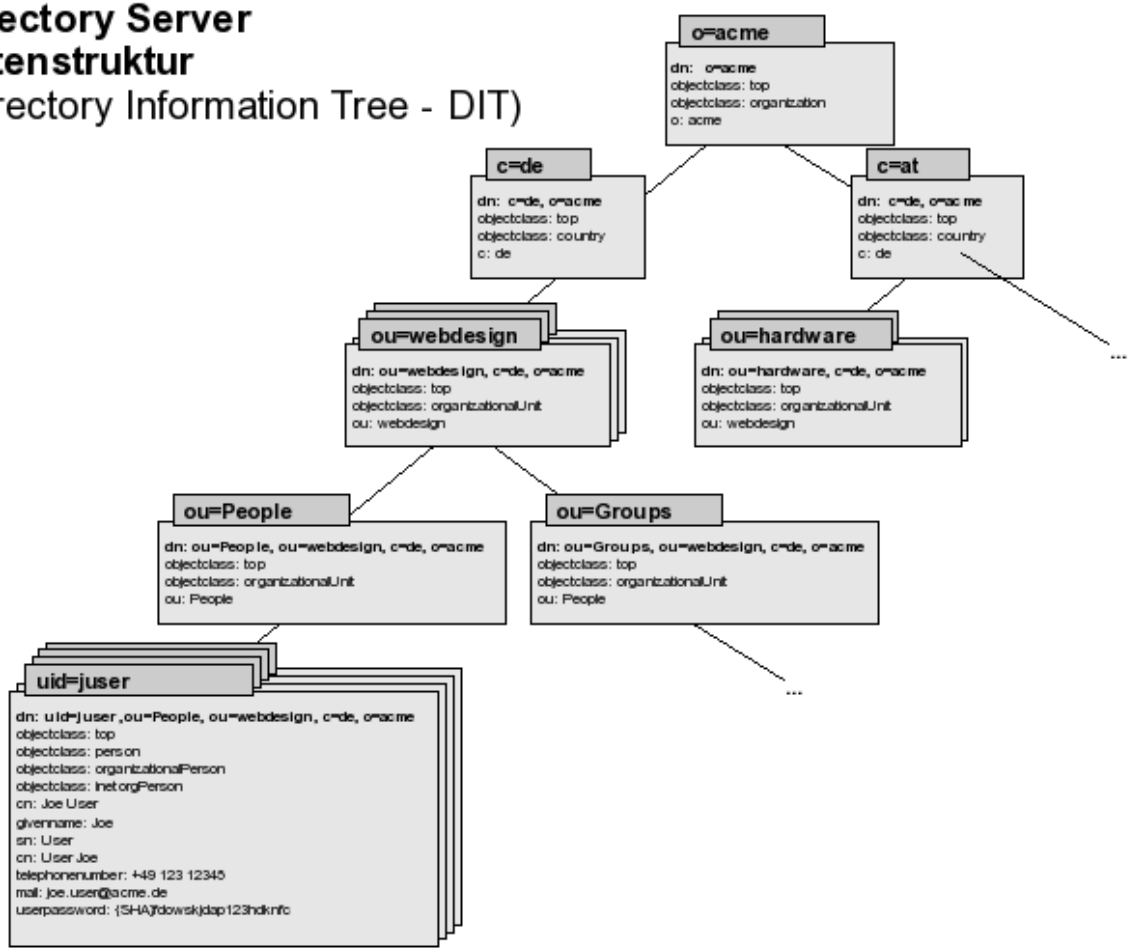
Verzeichnisdienste

Ein **Verzeichnisdienst** (englisch *directory service*) stellt in einem Netzwerk eine zentrale Sammlung an Daten bestimmter Art zur Verfügung. Die in einer hierarchischen Datenbank gespeicherten Daten können nach dem Client-Server-Prinzip verglichen, gesucht, erstellt, modifiziert und gelöscht werden. (Wikipedia, 8.11.2007)

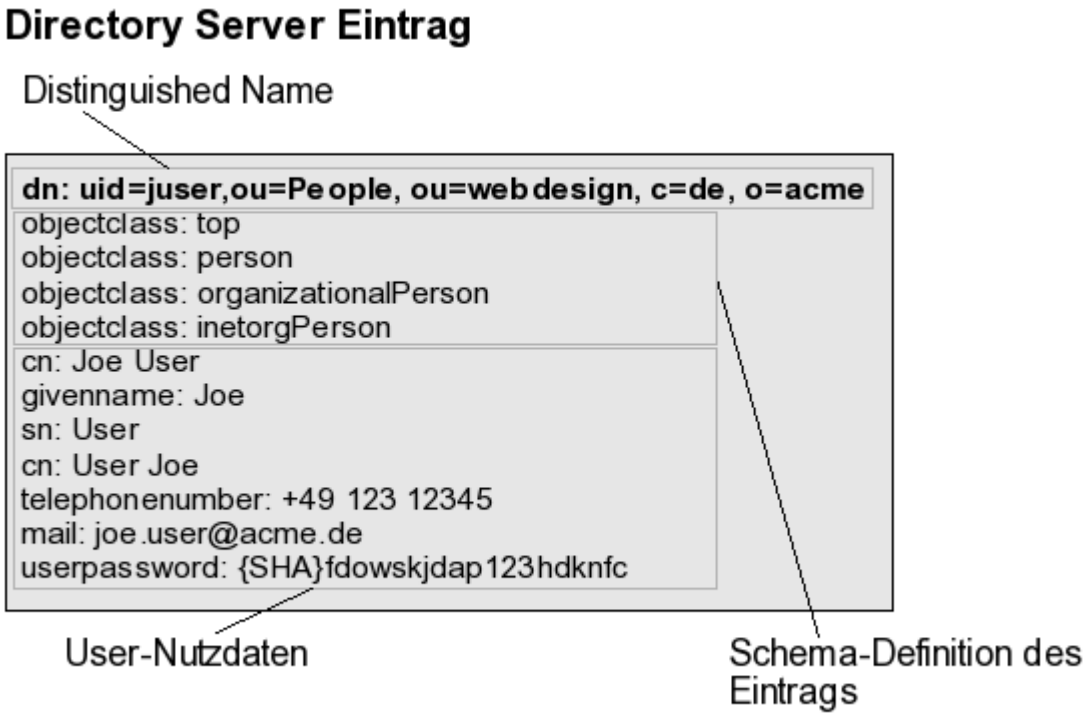
- Beispiele: Active Directory, eDirectory, NIS, Passport
- Protokoll: LDAP (Lightweight Directory Access Protocoll)

Verzeichnisdienste

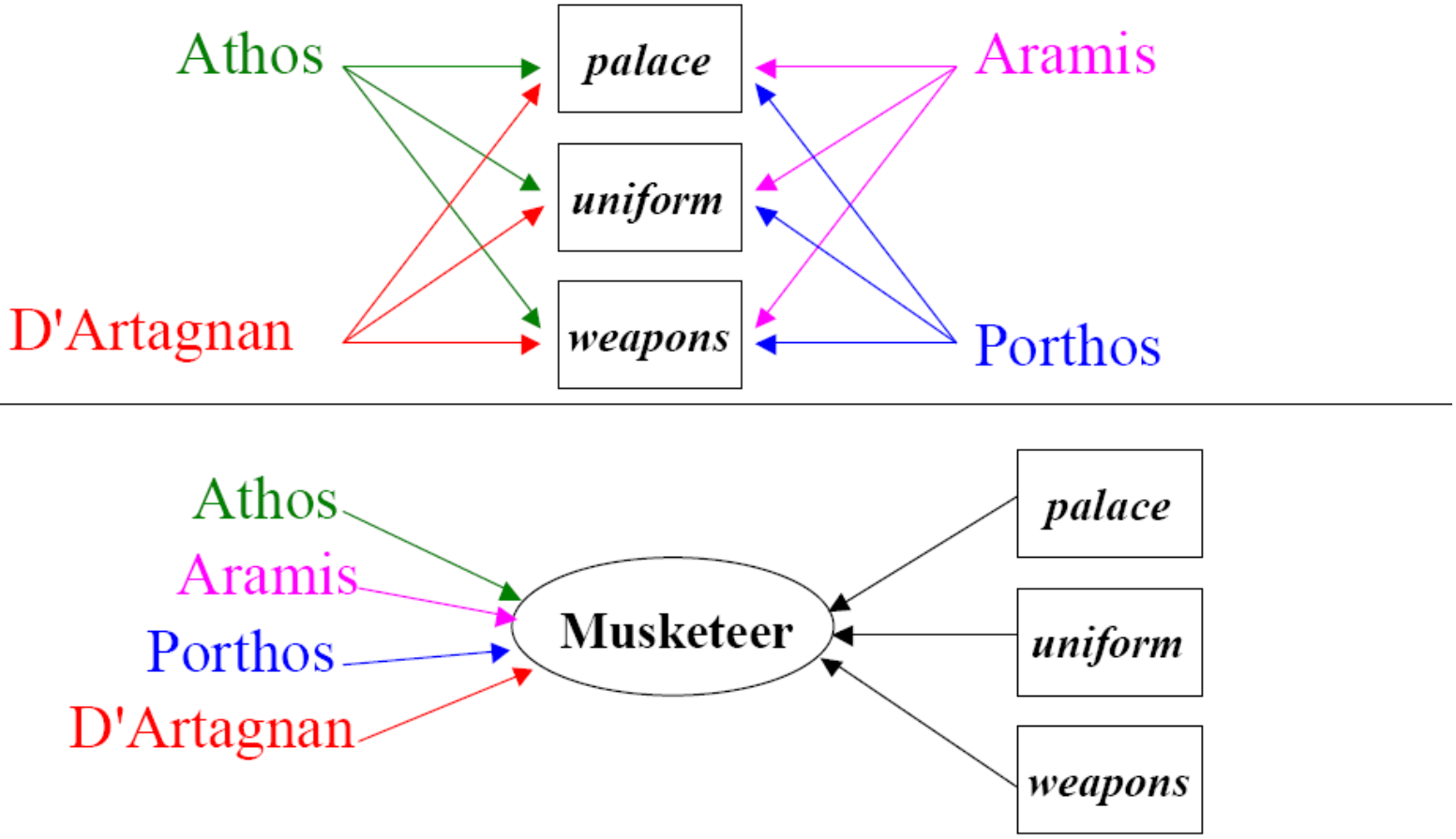
Directory Server
Datenstruktur
(Directory Information Tree - DIT)



Verzeichnisdienste



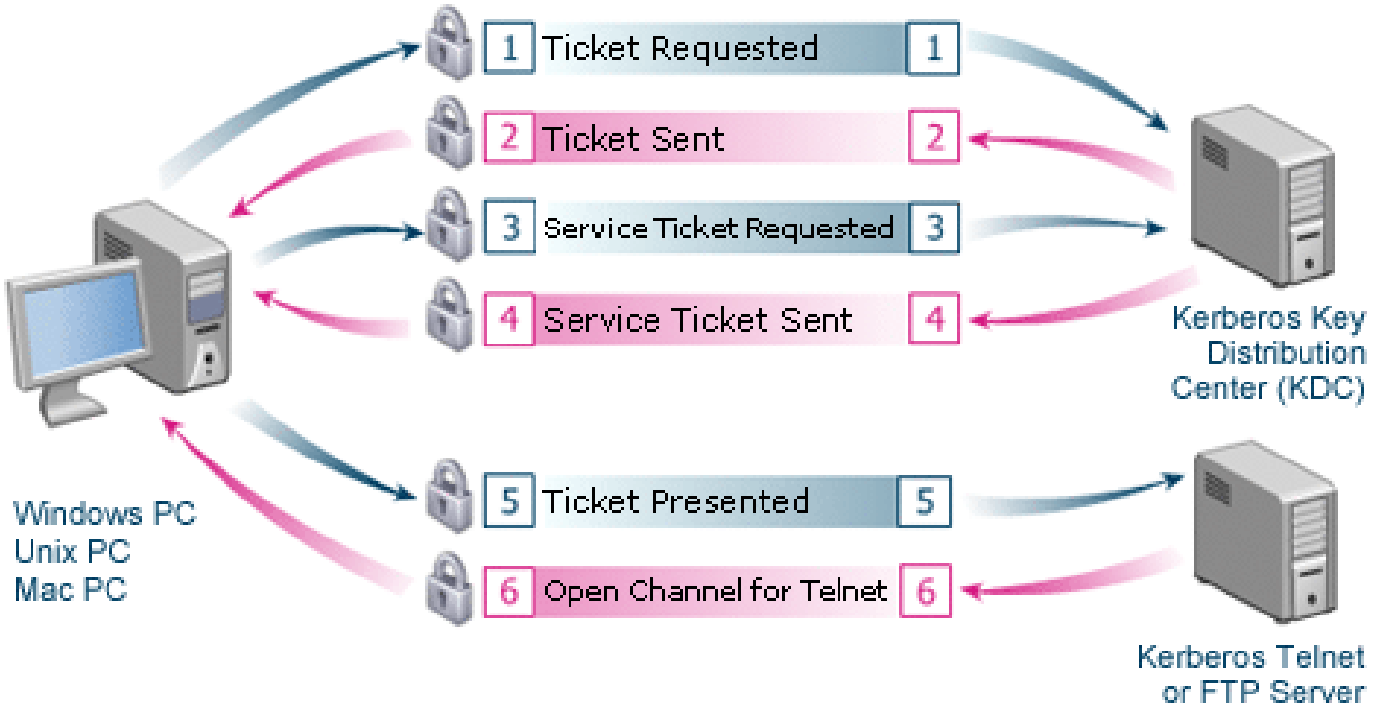
Role Based Access Control



Kerberos

- am MIT entwickelt (Project Athena)
- Versionen 1-3 rein intern, erst Version 5 erlangte große Beleibtheit
- Standard-Authentifizierungsschema in Active Directory und Mac OS X
- basiert auf Needham-Schröder Protokoll
- Probleme:
  - single point of failure
  - Zeit Synchronisation

Kerberos


1 Ticket Requested 1
2 Ticket Sent 2
3 Service Ticket Requested 3
4 Service Ticket Sent 4
Kerberos Key Distribution Center (KDC)
Windows PC
Unix PC
Mac PC
5 Ticket Presented 5
6 Open Channel for Telnet 6
Kerberos Telnet or FTP Server

Agenda

1. Die grundlegenden Fragen
    1. Identität
    2. Identitätsmanagement(-systeme)
    3. Authentifizierung & Autorisierung
2. Die Vergangenheit
    1. klassische Authentifikation
    2. Access Control Lists
3. Die Gegenwart
    1. Verzeichnisdienste
    2. verteile Authentifizierung
    3. Role Based Access Control
4. Die Wünsche für die Zukunft
    1. Trusted Source of Authority
    2. Single Sign-On
    3. Privacy
5. Die Hoffnungsträger
    1. federated Identity
        1. Shibboleth
    2. Identity 2.0
        1. OpenID
        2. Infromation Cards

Was wünscht Ihr euch für ein perfektes Identitätsmanagement?

Mindmap

Agenda

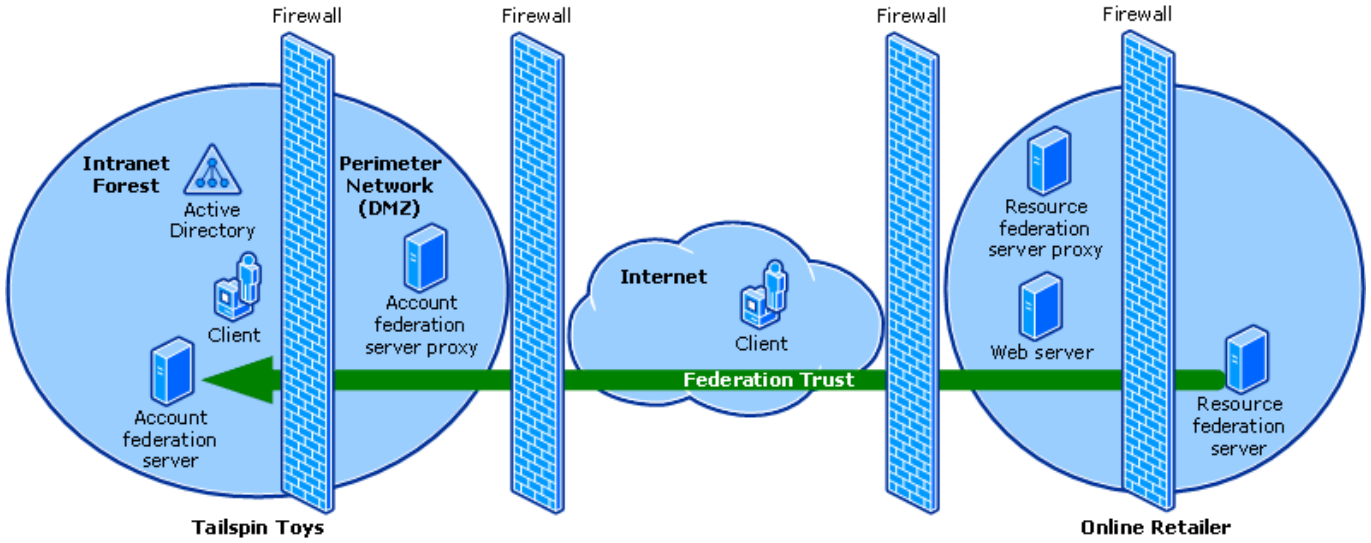
1. Die grundlegenden Fragen
    1. Identität
    2. Identitätsmanagement(-systeme)
2. Die Vergangenheit
    1. Authentifizierung – Was bedeuten Benutzername und Passwort
    2. Autorisierung – Wie werden Rechte verteilt
3. Die Gegenwart
    1. Verzeichnisdienste – Eine Möglichkeit der zentralen Verwaltung
    2. verteile Authentifizierung – Die Anfänge von Single Sign-On
4. Die Wünsche für die Zukunft
    1. Trusted Source of Authority
    2. Single Sign-On
    3. Privacy
5. Die Hoffnungsträger
    1. federated Identity
        1. Shibboleth
    2. Identity 2.0
        1. OpenID
        2. Information Cards

Die Hoffnungsträger

- verschiedene staatliche Ansätze:
  - elektronische Gesundheitskarte
  - einheitliche Steuernummer
- Integrationsbemühungen im Internet2 und der Industrie
  - ADFS
  - Shibboleth
- Web 2.0
  - OpenID
  - CardSpace

Federated Identity

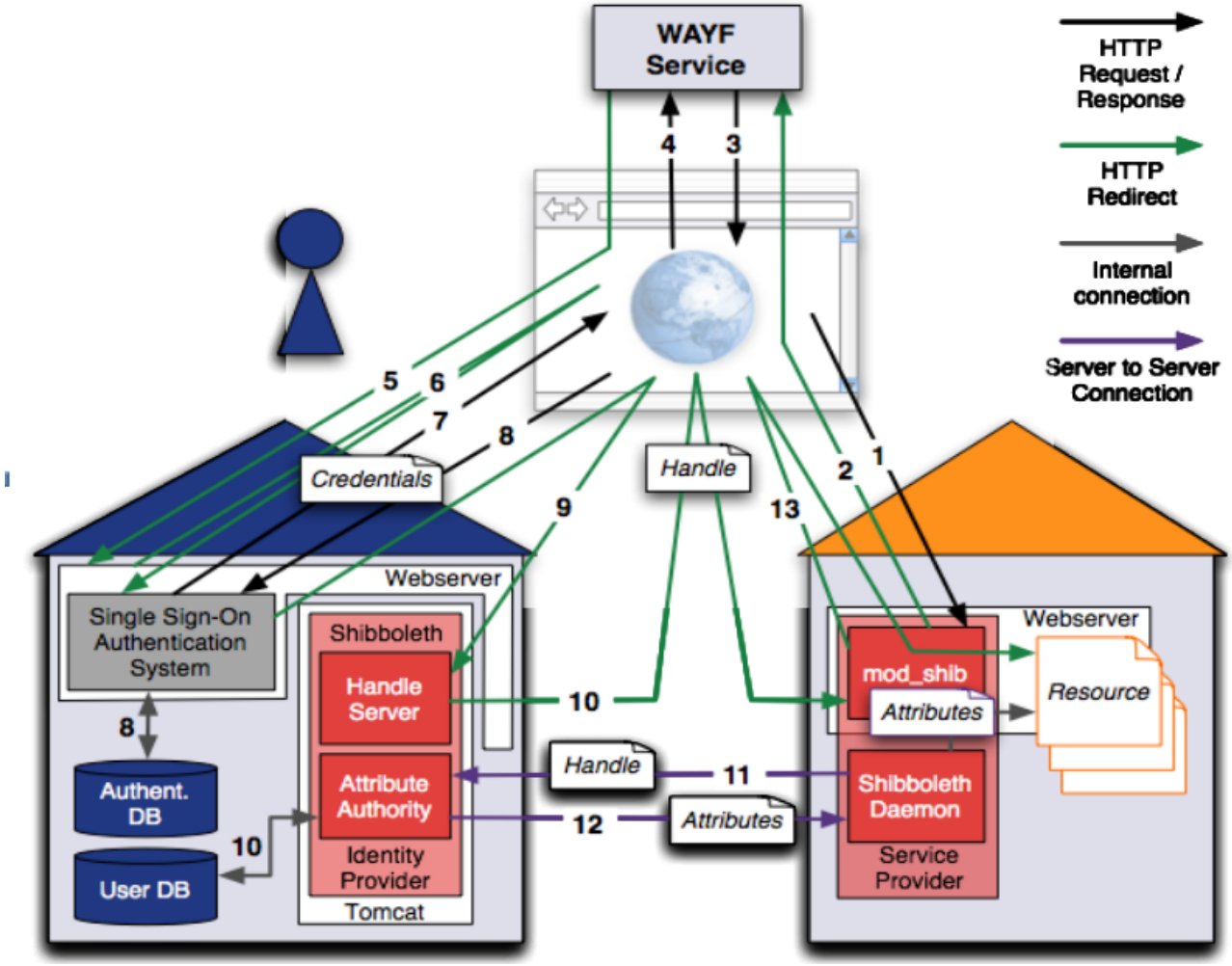
- zwei grundlegende Bedeutungen:
  - virtuelle Integration von Identity Management Systemen
  - Prozess der Benutzeranmeldung über verschiedene IT-Systeme bzw. Organisationen
- aufweichen der Grenzen zwischen IT-Systemen
- vermeiden von redundanter Datenhaltung



Shibboleth

- Komponente des Internet2
- basiert auf SAML
- verwendet durch DFN für die Identity-Integration der angeschlossenen Forschungseinrichtungen

Shibboleth


WAYF Service
HTTP Request / Response
HTTP Redirect
Internal connection
Server to Server Connection
4
3
5
6
7
8
9
10
11
12
13
1
2
Credentials
Handle
Webserver
Single Sign-On Authentication System
Shibboleth
Handle Server
Attribute Authority
Identity Provider
Tomcat
Authent. DB
User DB
Webserver
mod_shib
Attributes
Resource
Shibboleth Daemon
Service Provider

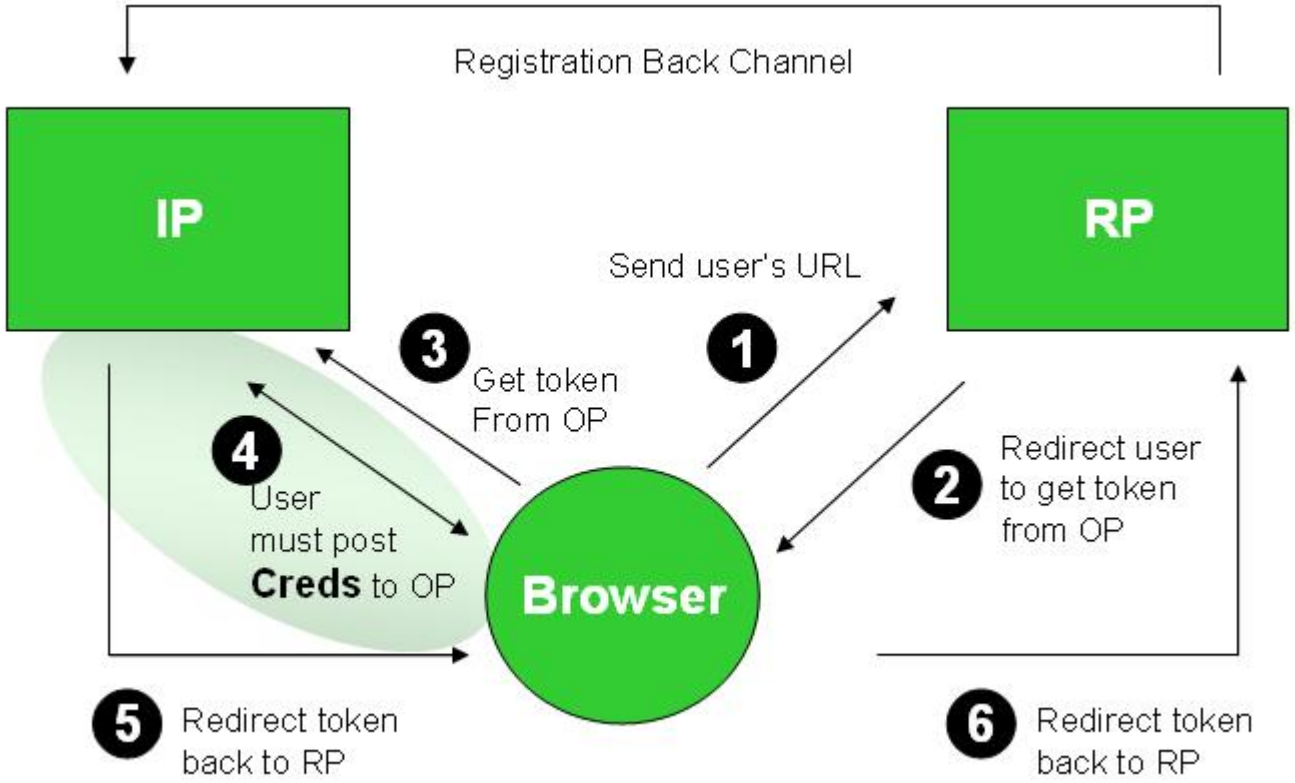
Identity 2.0

- Übertragung des federated Identity auf das Web
- aber: andere Schwerpunkte → user-centric IdM

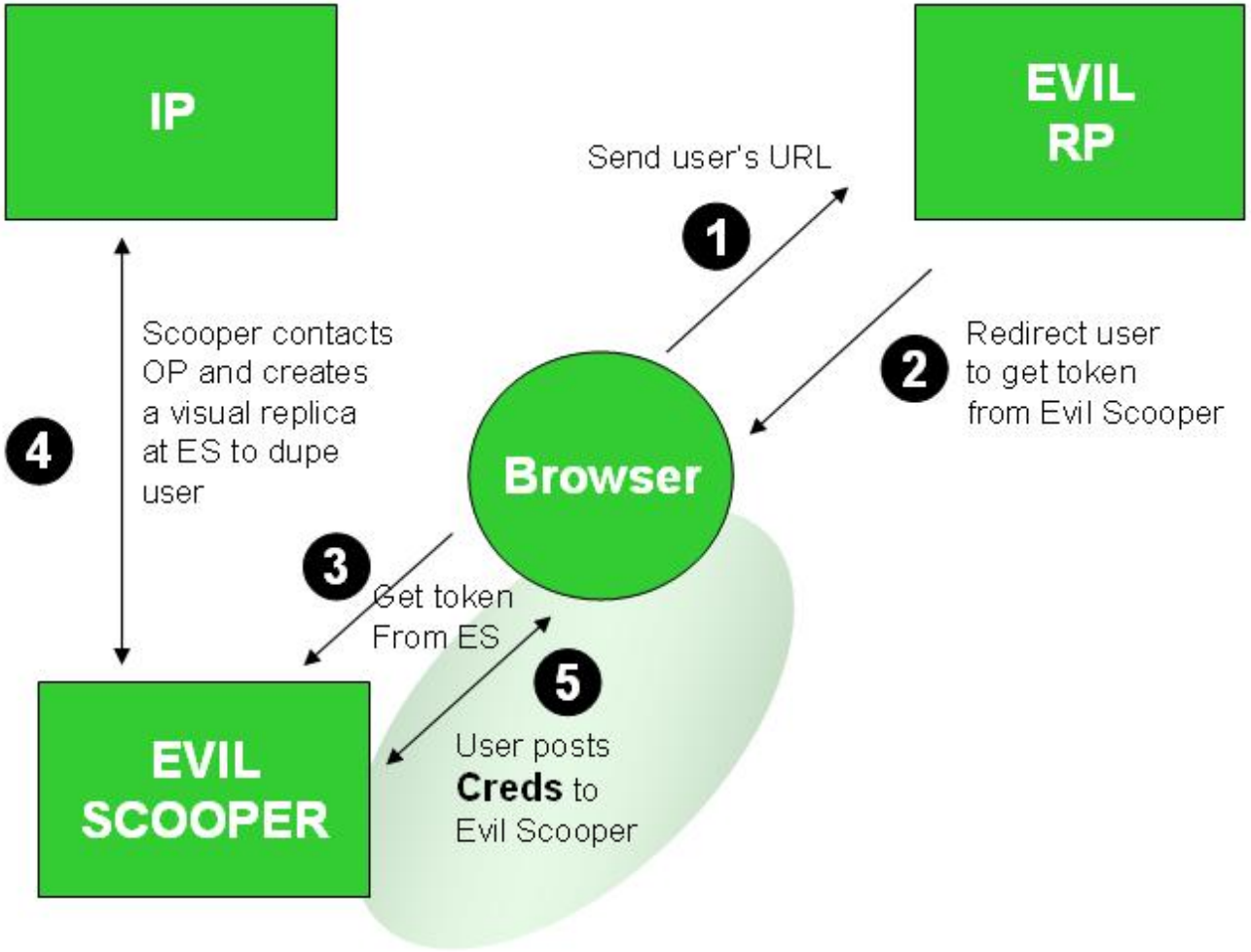
OpenID

- dezentrales Single Sign-On
- Support für Firefox 3 und Vista in Entwicklung
- Freiheit auf mehreren Ebenen:
  - Identität auf beliebigem Rechner hostbar
  - große Auswahl an Software-Komponenten
  - "OpenID does not crumble if any one company turns evil of goes out of business." (Brad Fitzpatrick)
  - offener Entwicklungsprozess
  - offen für eigene Ideen/Entwicklungen
- Nachteil: Phishing-Anfälligkeit bliebt bestehen

OpenID


Registration Back Channel
IP
RP
Send user's URL
1
3
Get token
From OP
4
User
must post
Creds to OP
Browser
2
Redirect user
to get token
from OP
5
Redirect token
back to RP
6
Redirect token
back to RP

OpenID


IP
EVIL RP
Send user's URL
1
2
Redirect user to get token from Evil Scooper
Scooper contacts OP and creates a visual replica at ES to dupe user
4
Browser
3
Get token From ES
5
EVIL SCOOPER
User posts **Creds** to Evil Scooper

Information Cards

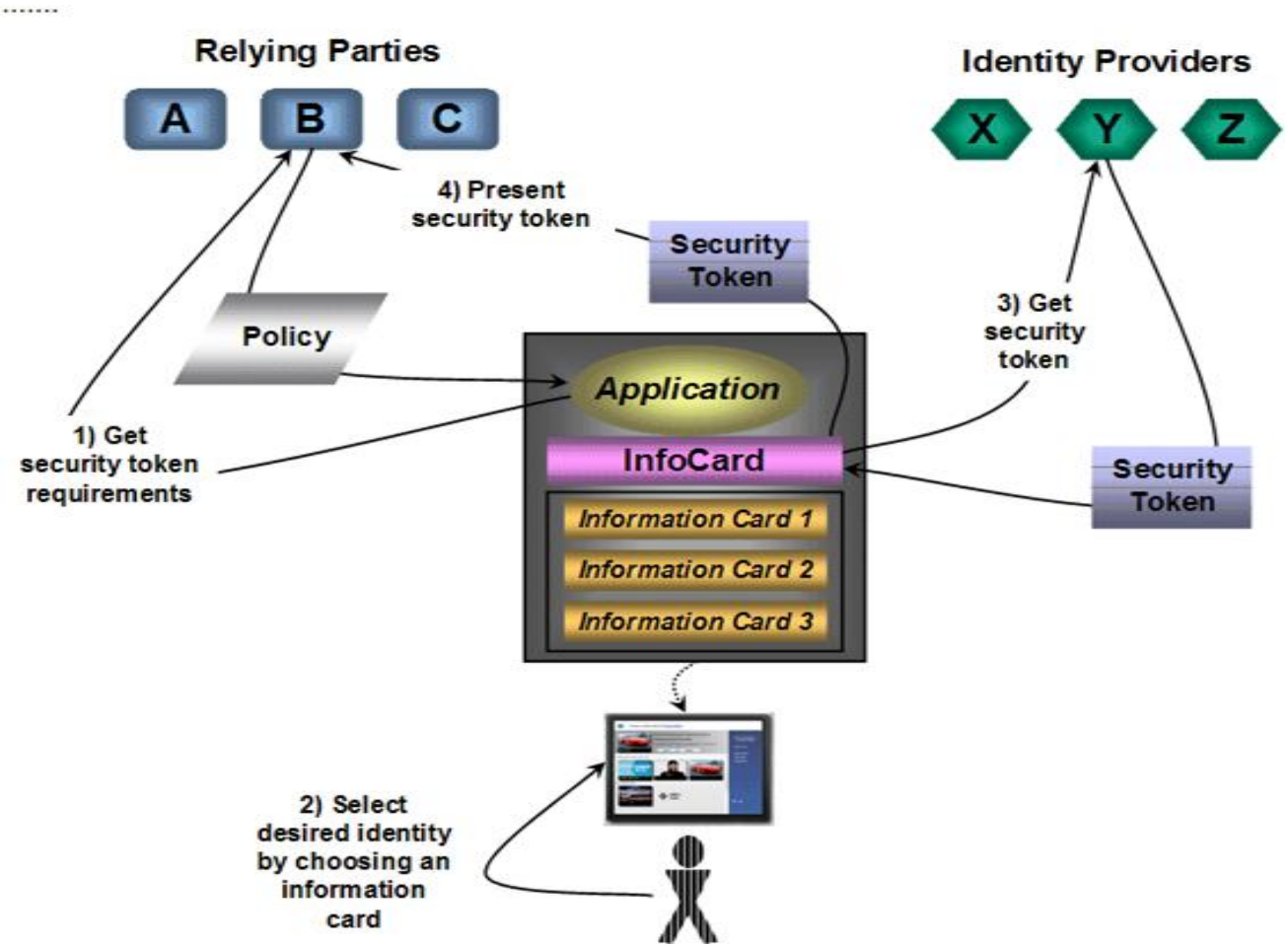
- Ziele für das "Identity Metasystem":
  - Unterstützung für jedes Identitymanagementsystem

    → Nutzung von offenen Protokollen (WS-*)
  - durchgehende Benutzerkontrolle

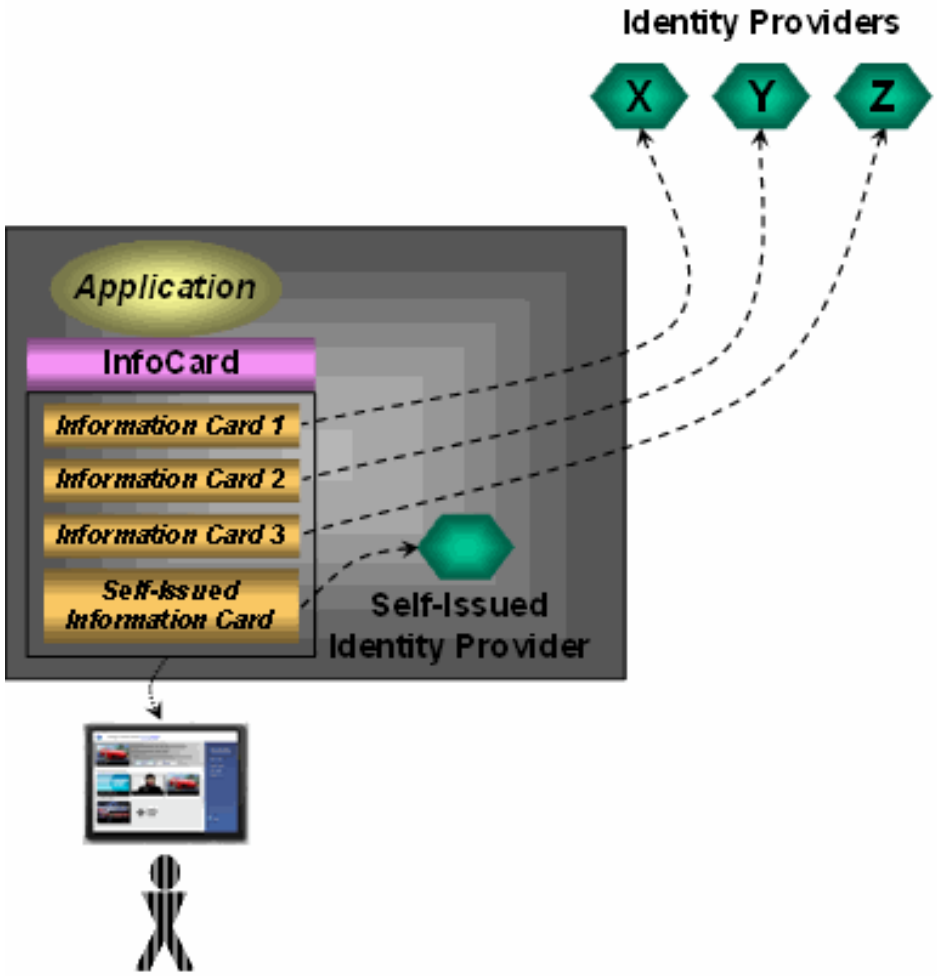
    → keine direkte Kommunikation zwischen IdP und RP
  - Ersatz für Passwörter

    → keine Annahmen über die Art der Identität
  - Erhöhung der Benutzerzufriedenheit

Information Cards



Information Cards



Information Cards

Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

Vielen Dank für Ihre Aufmerksamkeit

Quellen

Vorlesung Kommunikationssystem I

http://(en|de).wikipedia.org

https://www.prime-project.eu/prime_products/presentations/idmanage-berlin-20060913.pdf

http://blog.thomasbiesenbach.de/uploads/diverses/SL_biesi_14062007_1_300.jpg

http://www.opengroup.org/security/heron.pdf

http://www4.informatik.uni-erlangen.de/Lehre/SS02/PS_KVBK/talks/folien_guido.pdf

http://oskorei.motpol.nu/?p=127

http://www.ericom.com/kerberos.asp

http://www.identityblog.com/

http://blogs.zdnet.com/digitalID/?p=78