

Selected Topics IT-Security 1

Identity Management

felix.hoerandner@iaik.tugraz.at

Felix Hörandner

Graz, October 2019



EGIZ


E-Government Innovationszentrum

Das E-Government Innovationszentrum ist eine
gemeinsame Einrichtung des Bundeskanzleramtes
und der TU Graz



BUNDESKANZLERAMT  ÖSTERREICH

Overview

5'	 Structure, Learning Targets	Presentation
20'	General Definitions <ul style="list-style-type: none">• Identity, Digital Identity, Electronic Identity• Identification, Authentication, Authorization• Identity Types, Threats, Challenges	Presentation
10'	Self-check: General Definitions	Groups of 2-3: Discussion Presenter: Shows solution
10'	Identity Management <ul style="list-style-type: none">• Identity Management Lifecycle• Identity Management Models	Presentation
10'	Self-check: Identity Management	Groups of 2-3: Discussion Presenter: Shows solution
15'	Identity Protocols <ul style="list-style-type: none">• Generic• SAML• OpenID Connect• OAuth	Presentation
10'	Self-check: Identity Protocols	Groups of 2-3: Discussion Presenter: Shows solution
10'	Research: CREDENTIAL	Presentation

Learning Targets: General Definitions

The student is able to...

- » ... **explain** the terms **digital identity** and **electronic identity**, and **explain** their **components** as well as their **differences**
- » ... **explain** the terms **identification**, **authentication** and **authorization**, and **give examples** for each.
- » ... **explain** and **classify authentication mechanisms**.
- » ... **explain** and **classify identity types, challenges and threats** .

Learning Targets: Identity Management

The student is able to...

- » ... **explain** the **identity management lifecycle**, **explain** and **enumerate** its **stages**, and **apply** it to a real world scenario
- » ... **explain** the **stakeholders** in identity management and **explain** their **interconnections**
- » ... **explain** the individual **identity management models** and **explain** their **differences**

Learning Targets: Identity Protocols

The student is able to...

- » ... **explain** the **generic concept of identity protocols** and **enumerate** the sequence of **protocol steps**.
- » ... **explain** the **advantages** of using an identity protocol.
- » ... **explain** the **differences** between selected identity protocols.
- » ... **apply the identity protocol (steps)** to a selected use case.

Overview

- » **General Definitions**
 - » Identity, Digital Identity, Electronic Identity
 - » Identification, Authentication, Authorization
 - » Identity Types, Threats, Challenges
- » **Identity Management**
 - » Identity Management Lifecycle
 - » Identity Management Models
- » **Identity Protocols**
 - » SAML, OAuth, OpenID Connect

Overview

» General Definitions

- » Identity, Digital Identity, Electronic Identity
- » Identification, Authentication, Authorization
- » Identity Types, Threats, Challenges

» Identity Management

- » Identity Management Lifecycle
- » Identity Management Models

» Identity Protocols

- » SAML, OAuth, OpenID Connect

Identity

“who a person is, or the qualities of a person or group that make them different from others”

[Cambridge Online Dictionaries]

“the fact of being who or what a person or thing is”

”the characteristics determining who or what a person or thing is”

[Oxford Dictionaries]

- » **Describes a person’s unique and distinctive characteristics**
- » **Distinguishes one from another**
 - » **E.g.: Name, gender, color of hair and eyes, ...**
- » **In real life also referred to as *principal***
- » **Within a digital context as *subject***

Digital Identity

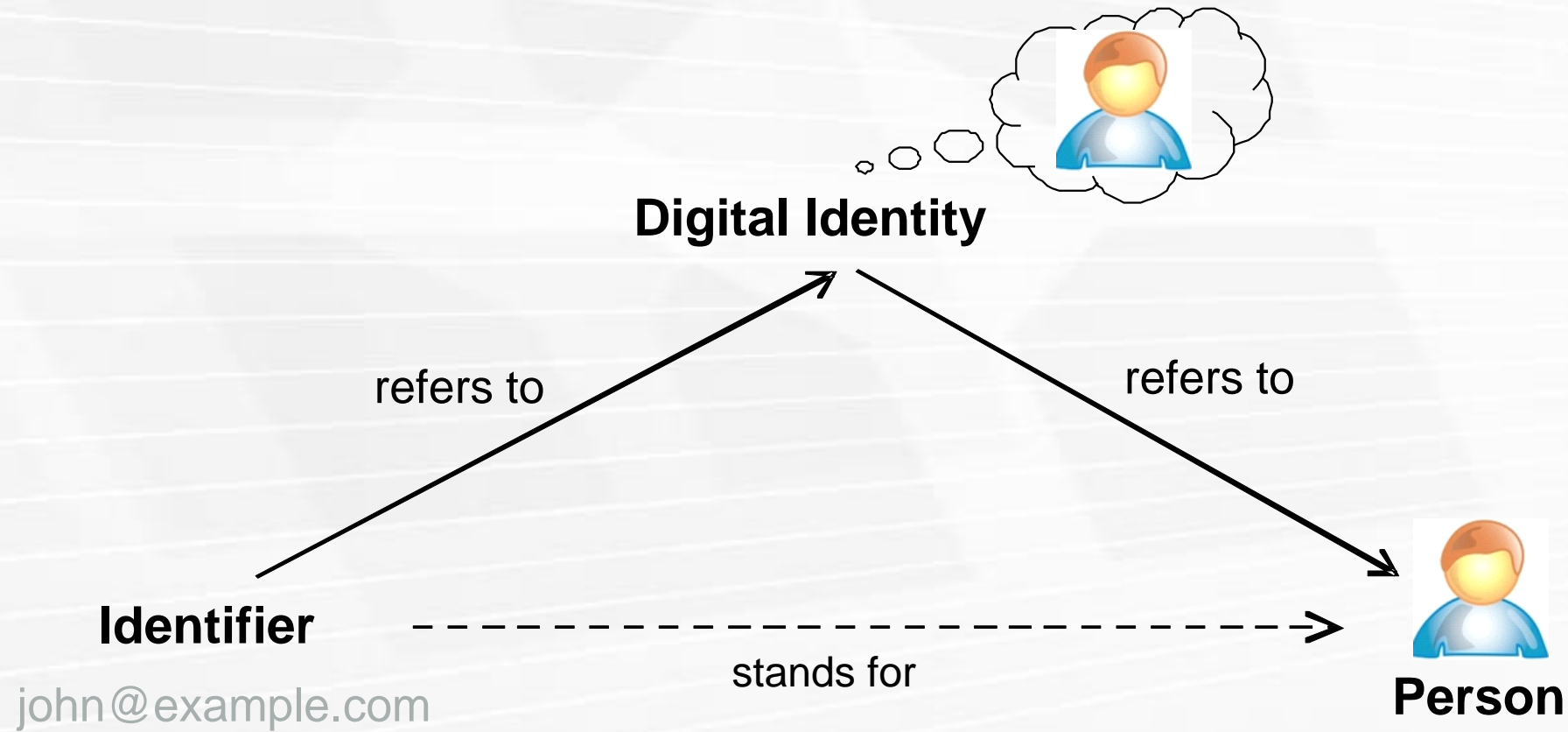
“Digital identity can be defined as the digital representation of the information known about a specific individual or organization. [Bertino and Takahashi]

„A Digital Identity is the representation of a human identity that is used in a distributed network interaction with other machines or people.“ [DigitalID World magazine]

“In an identity management system identity is that set of permanent or long-lived temporal attributes associated with an entity.” [Camp]

- » **Same identity properties and attributes, but digitally available**
 - » E.g.: name, date of birth, ...
 - » Also: username, e-mail, ...
- » **Applicable also to non-natural persons**
 - » E.g.: computer system, company, ...

Digital Identity | Triangle



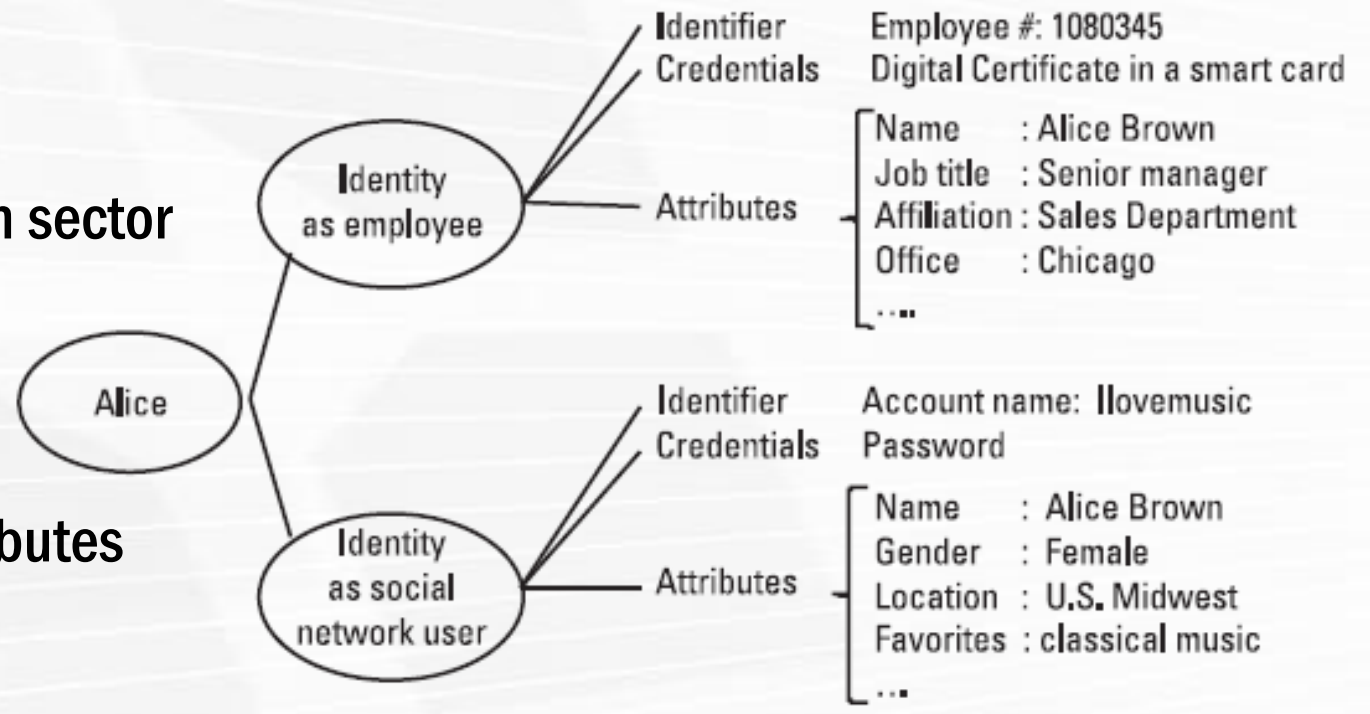
Ref: GINI-SA

Digital Identity | Parts

- » **Identifier**
 - » Character string identifying a person
 - » May be restricted in time or application sector
 - » E.g.: username, e-mail, URI, ssPIN, ...

- » **Credentials**
 - » Used for proving identifier and/or attributes
 - » E.g.: password, certificate, ...

- » **Attributes**
 - » Describing a person's properties
 - » E.g.: name, date of birth, gender, ...



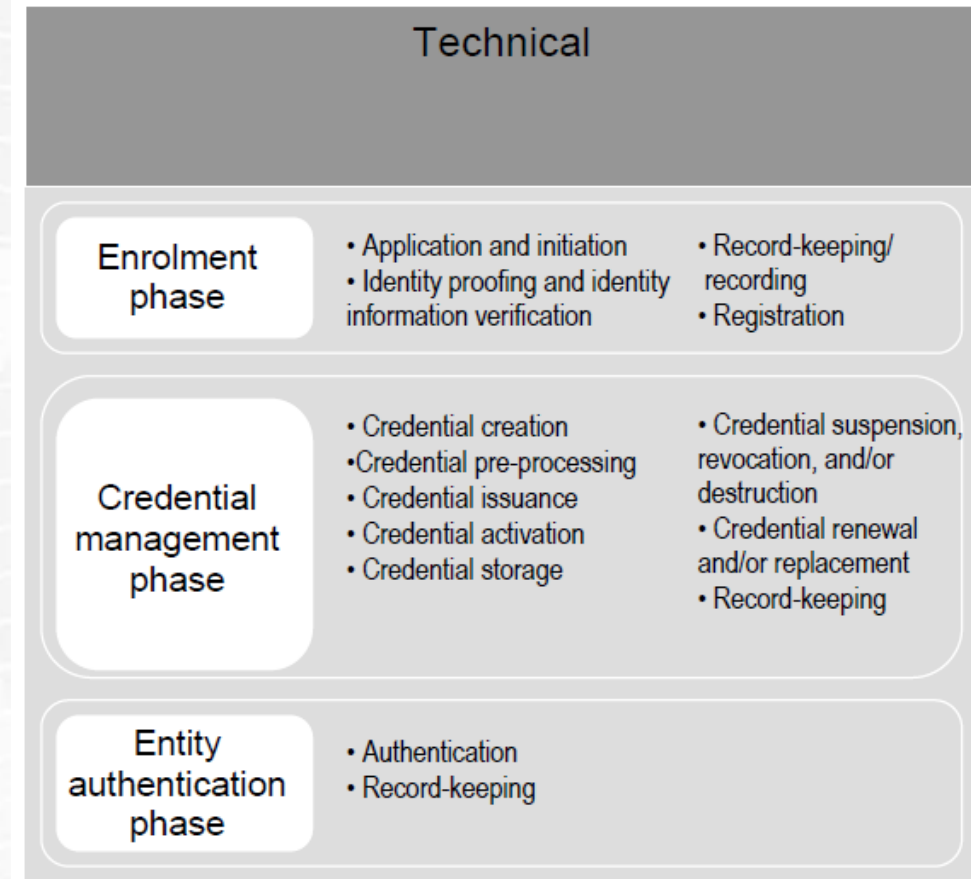
Ref: Bertino/Takahashi

Electronic Identity (eID)

- » Aims to guarantee the unique identity of a (natural or legal) person
- » Ensure trust between parties involved in electronic transactions
- » Features that need to be supported by an eID
 - » Universality of coverage (everyone)
 - » Uniqueness, Exclusivity (one and only one)
 - » Permanence (permanently)
- » Particularly required in sensitive areas of applications
 - » E.g.: e-Government
 - » Identification, Signature, Authentication

Levels of Assurance

- » Assurance level of the transmitted identity data
- » Quantitative representation of
 - » Identity enrolment
 - » Credential management
 - » Authentication process, etc.
- » Applications define required minimum level
- » Different, but related approaches
 - » ISO/IEC 29115: Levels of Assurance (4 levels)
 - » eIDAS: Levels of Assurance (3 levels)



ISO/IEC 29115

Overview

» General Definitions

- » Identity, Digital Identity, Electronic Identity
- » **Identification, Authentication, Authorization**
- » Identity Types, Threats, Challenges

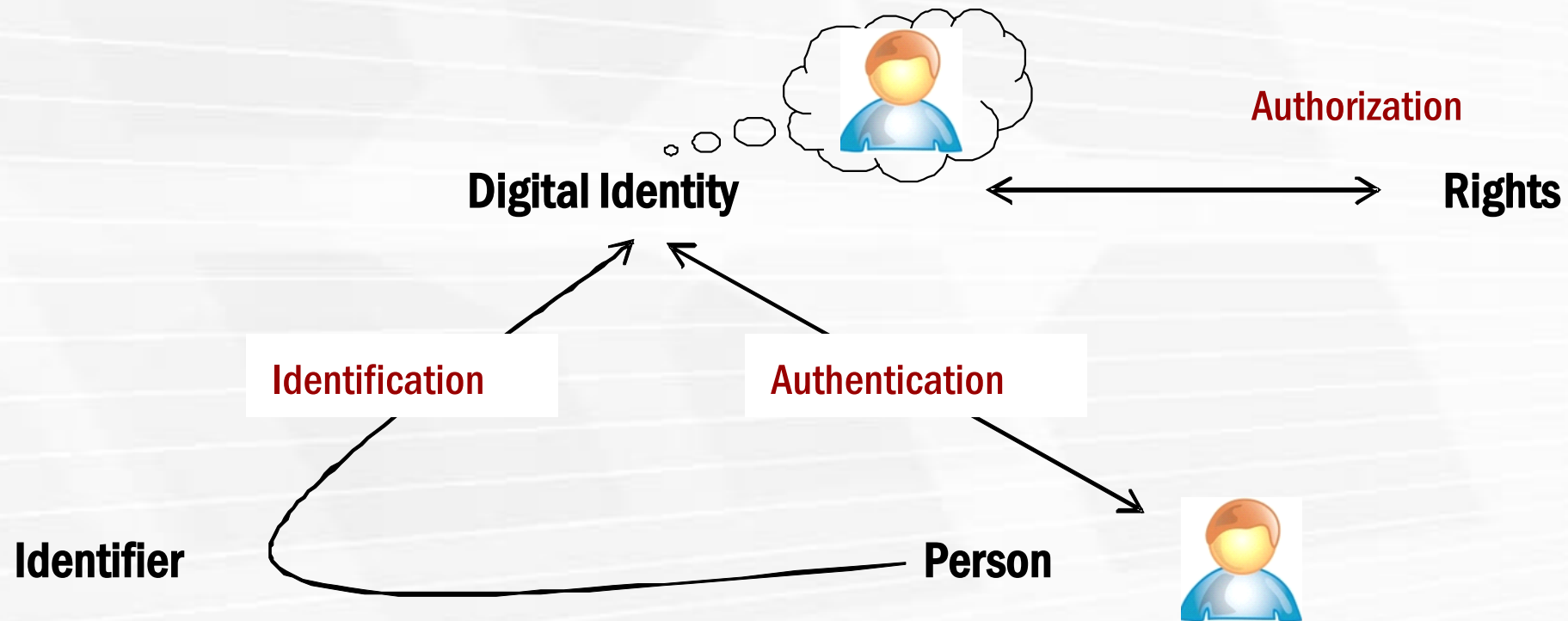
» Identity Management

- » Identity Management Lifecycle
- » Identity Management Models

» Identity Protocols

- » SAML, OAuth, OpenID Connect

Identification | Authentication | Authorization

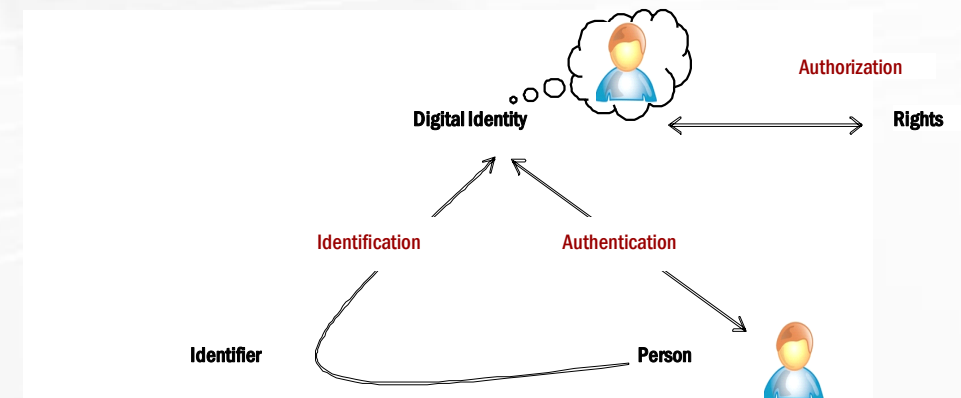


Identification

Identification is the association of a personal identifier with an individual presenting attributes.

[Clarke]

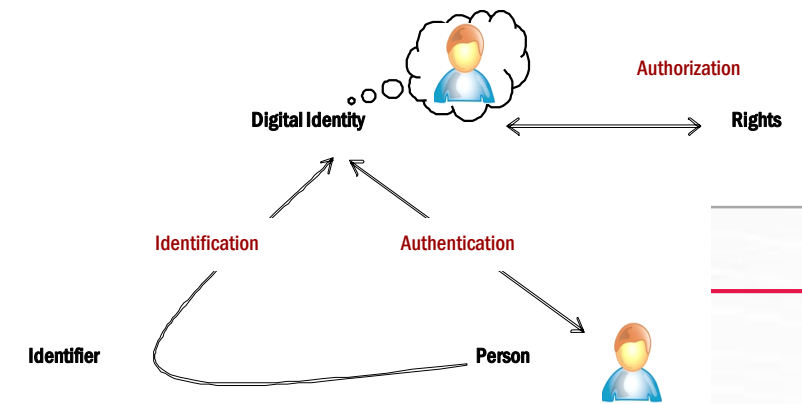
- » **Association between one/more personal attributes and an individual**
 - » E.g.: the name “Max Mustermann” identifies the person “Max Mustermann”
- » **Unique identification**
 - » If no other person’s name is “Max Mustermann” (within the context)
 - » Else additional attributes are required (e.g. date of birth, address, ...)
- » **Traditional: ID card**
 - » E.g.: Passport, identification card, driving license, ...
- » **Online: Electronic ID (eID)**
 - » E.g.: Austrian Citizen Card



Means of Identification

Option	Description	Example
Appearance	How the person looks	Color of skin or eyes, gender, ... Pictures on ID documents
Social behavior	How the person interacts with others	Voice, body language, ... Mobile phone records, video surveillance data, credit card transactions, etc.
Names	How the person is called by other people	Family name, name listed in national registry or on passports, nicknames
Codes	How the person is called by an organization	Social security number, matriculation number, ID card numbers
Knowledge	What the person knows	Password, PIN
Tokens	What the person has	Driving license, passport, smart card, mobile phone
Bio-dynamics	What the person does	Pattern of handwritten signature
Natural physiography	What the person is	Fingerprint, retina, DNA
Imposed physical characteristics	What the person is now	Height, weight, rings, necklaces, tattoos

Authentication



Authentication is proof of an attribute. [Clarke]

Authentication of identity is proving an association between an entity and an identifier. [Clarke]

The process of verifying a subject's identity or other claim, e.g. one or more attributes. [GINI-SA]

- » Process of proving a person's claimed identity or digital identity
- » Traditional:
 - » Proof of identity (name, appearance, ...) e.g. by passport
- » Online:
 - » Proof of identity (username) e.g. using a password

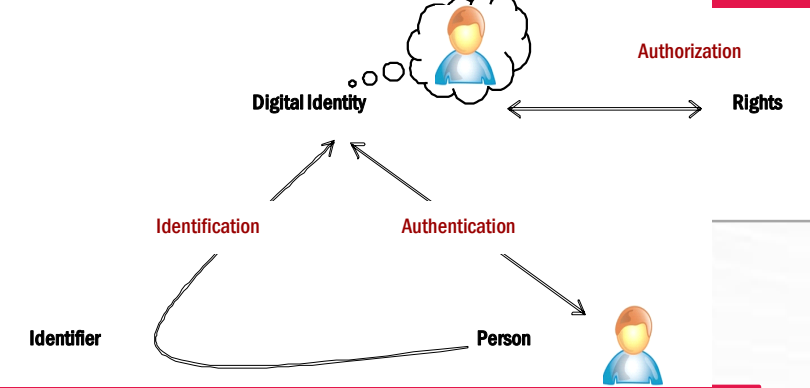
Authentication Mechanisms

- » **Knowledge: “Knowing something”**
 - » Authentication based on presented knowledge
 - » E.g., password, PIN, ...
- » **Possession: “Having something”**
 - » Authentication based on “something” an entity owns or has for proving her identity.
 - » E.g., passport, smart card, private key, ...
- » **Physical Property: “Being something”**
 - » Authentication based on a physical property
 - » E.g., fingerprint, ...
- » **Behavior Pattern: “Doing something”**
 - » Authentication based on something an entity does
 - » E.g., voice recognition, ...

Multi-Factor-Authentication

- » **Combining different authentication mechanisms to increase security**
- » **E.g. Ownership and Knowledge (2-factor)**
 - » **Citizen card: smart card + PIN**
 - » **Mobile phone signature: mobile phone + password**

Authorization



Authorization is a decision to allow a particular action based on an identifier or attribute. [Clarke]

Through authorization, rights are assigned to a digital identity. [GINI-SA]

- » Usually carried out after an authentication process
- » Assigning/Enforcing access rights for resources to entities
 - » E.g.: Read/write rights on file system
- » Often based on roles or groups
 - » E.g.: doctor, student, admin, ...

Overview

» General Definitions

- » Identity, Digital Identity, Electronic Identity
- » Identification, Authentication, Authorization
- » Identity Types, Threats, Challenges

» Identity Management

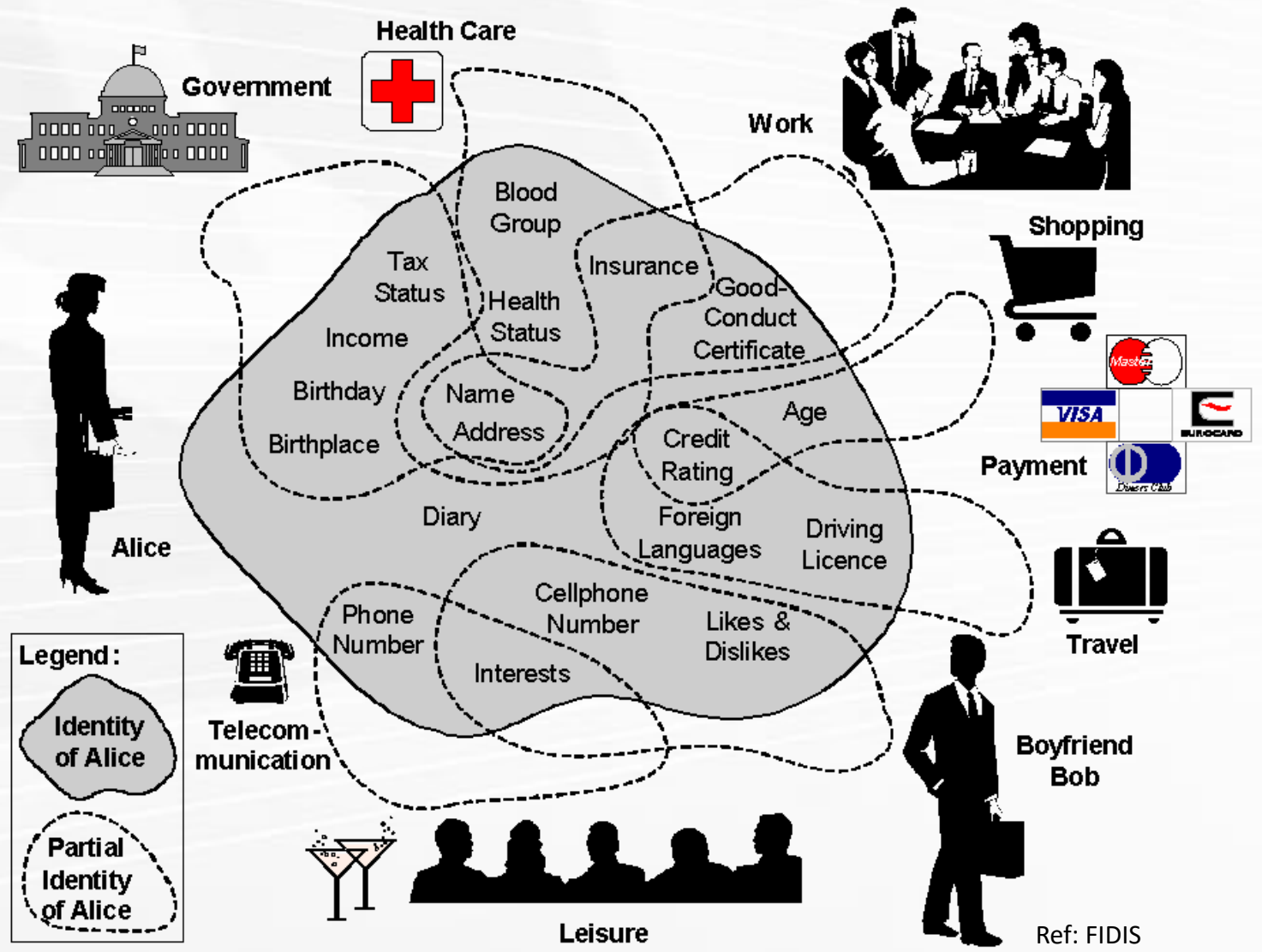
- » Identity Management Lifecycle
- » Identity Management Models

» Identity Protocols

- » SAML, OAuth, OpenID Connect

Identity Types | Complete, Partial

- « Complete identity
 - « All attribute values of all identities of this person
- « Partial identities
 - « Different set of attributes forming identities
 - « E.g.: at work, social media, ...



Identity Types | Pseudonymous, Anonymous

» Pseudonymous identities

- » Trustworthy entity decouples the digital identity from real person
- » Only it can link pseudonym to real person
- » E.g. name changed by editorial office

» Anonymous identities

- » Completely decouples digital identity from real person
 - » Unlinkable
- » Usually temporary and for single transactions
 - » E.g.: completing a question form

Identity Types | Local, Global, Federated, Brokered

- » **Local identity**
 - » Valid only within a closed environment
 - » E.g.: Windows PC
- » **Global identity**
 - » Valid within a wider context
 - » E.g.: Passport
- » **Federated identity**
 - » Identity data shared and linked over multiple systems
 - » Single sign-on (SSO)
- » **Brokered identity**
 - » Identity translation
 - » E.g.: Transform partial identity to pseudonymous identity for privacy reasons

Identity Threats

- » **Identity linking**
 - » Information regarding an identity is collected from one/more services
 - » E.g.: Persistent identifiers, personal details in social networks, requesting more information than needed, selling personal data
- » **Identity theft**
 - » One person claims to be another person
 - » E.g.: Social engineering, eavesdropping communication, credit card fraud
- » **Identity manipulation**
 - » An identity's attributes are changed with intent
 - » E.g.: Modification of access rights
- » **Identity disclosure**
 - » An identity's attributes are disclosed
 - » E.g.: Intentionally or unintentionally disclosure of health data

Ref: Tsoikas/Schmidt

Challenges for Digital Identity

- » **Security**
 - » To encounter any identity threat or identity compromise
- » **Privacy**
 - » Minimal disclosure, anonymity, unlinkability
- » **Trust**
 - » Trust relationships between all involved entities/stakeholders are essential
- » **Data control**
 - » Users should be entitled to maximum control over their own personal data
- » **Usability**
 - » Easy-to-understand and usable authentication mechanism
- » **Interoperability**
 - » Facilitates the portability of identities
 - » Acceptance of different authentication mechanisms

General Definitions | Summary

- » **Identity:** “Max Mustermann“
- » **Digital Identity Parts:** Identifier, Credentials, Attributes
- » **Digital vs eID:** eID is unique

- » **Identification:** “I am Max Mustermann“
- » **Authentication:** “My passport proves that I am Max Mustermann”
- » **Authorization:** “As employee of company B, Max Mustermann is allowed to access Service A”

- » **Identity Types:** Complete, Partial; Pseudonymous, Anonymous; Local, Global, Federated, ...
- » **Identity Threats:** Linking, Theft, Manipulation, Disclosure
- » **Identity Challenges:** Security, Privacy, Trust, ...

Overview

- » **General Definitions**
 - » Identity, Digital Identity, Electronic Identity
 - » Identification, Authentication, Authorization
 - » Identity Types, Threats, Challenges
- » **Identity Management**
 - » **Identity Management Lifecycle**
 - » Identity Management Models
- » **Identity Protocols**
 - » SAML, OAuth, OpenID Connect

Identity Management (IdM)

Identity and access management combines processes, technologies, and policies to manage digital identities and specify how they are used to access resources. [Microsoft]

- » **Managing identities**
- » **Managing access rights for resources**
- » **Management of the identity lifecycle**
- » **Different dimensions**
 - » **E.g. within a system (e.g. company), network or country**

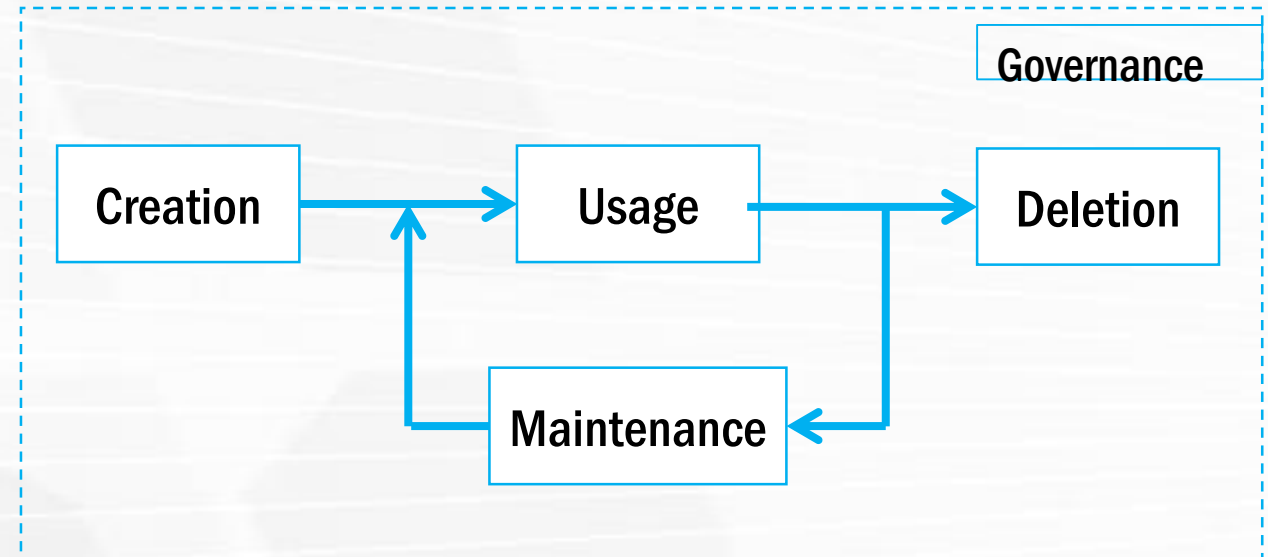
Identity Management Lifecycle | Creation, Usage

» Creation

- » Create data record of digital identity
 - » Contains different attributes (self-declared or proved and verified)
- » Credential is issued

» Usage

- » Used in different services
- » Authentication and authorization
- » Single sign-on (SSO)



Ref: Bertino/Takahashi

Identity Management Lifecycle | Maintenance, Deletion

» Maintenance

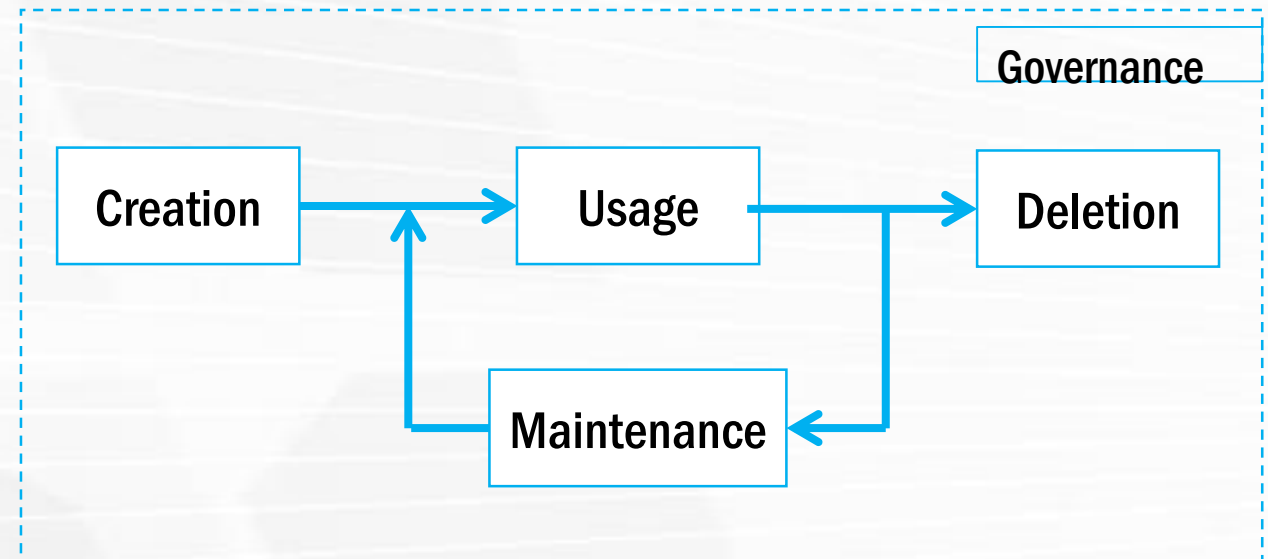
» Attributes may

- » Be added or deleted
- » Change (e.g. address)
- » Expire (e.g. certificate valid for 1 year)

» Identifiers should not be changed

» Deletion

- » Manual deletion
- » Expiration (e.g. validity period of certificate)
- » Revocation (e.g. employee leaves company)
- » Should be documented and other systems should be informed

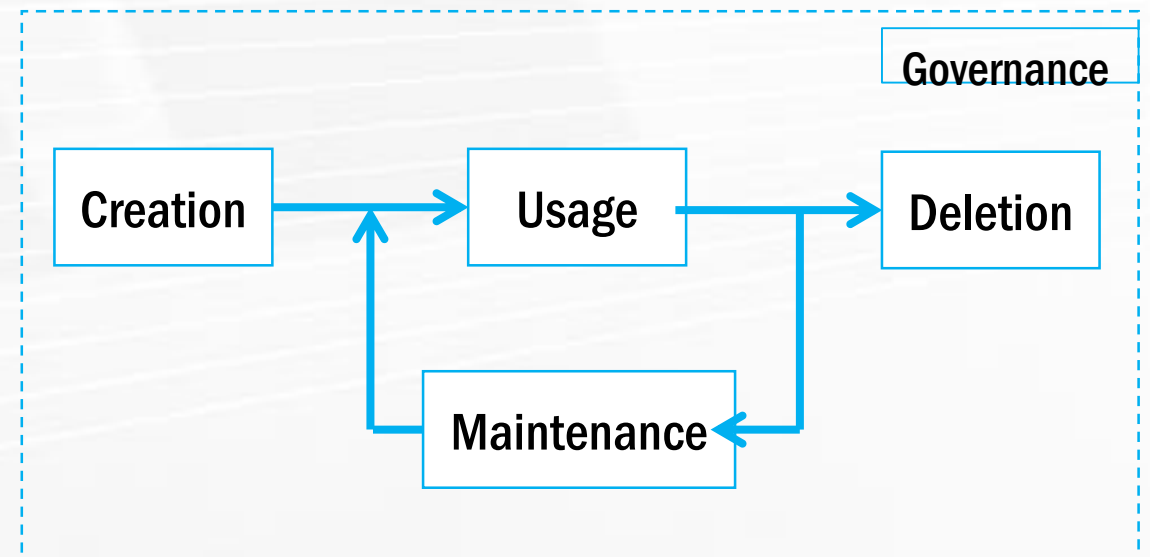


Ref: Bertino/Takahashi

Identity Management Lifecycle | Governance

» Governance

- » Policies/guidelines for
 - » creation, usage, maintenance, and deletion of identities
 - » authentication (e.g. authentication level/strength)
 - » authorization (e.g. conditions for data access)
- » Audit/traceability of single activities
- » Often based on a legal framework



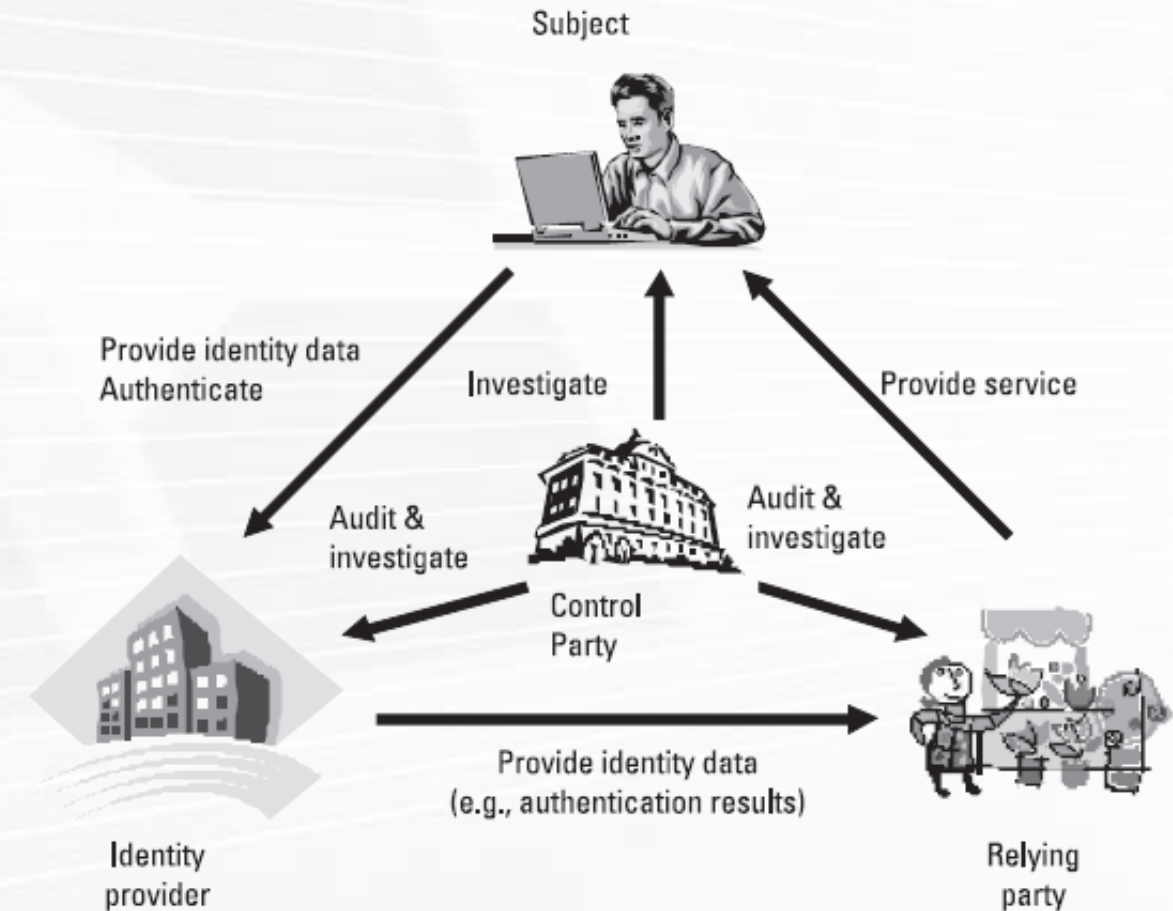
Ref: Bertino/Takahashi

Overview

- » **General Definitions**
 - » Identity, Digital Identity, Electronic Identity
 - » Identification, Authentication, Authorization
 - » Identity Types, Threats, Challenges
- » **Identity Management**
 - » Identity Management Lifecycle
 - » **Identity Management Models**
- » **Identity Protocols**
 - » SAML, OAuth, OpenID Connect

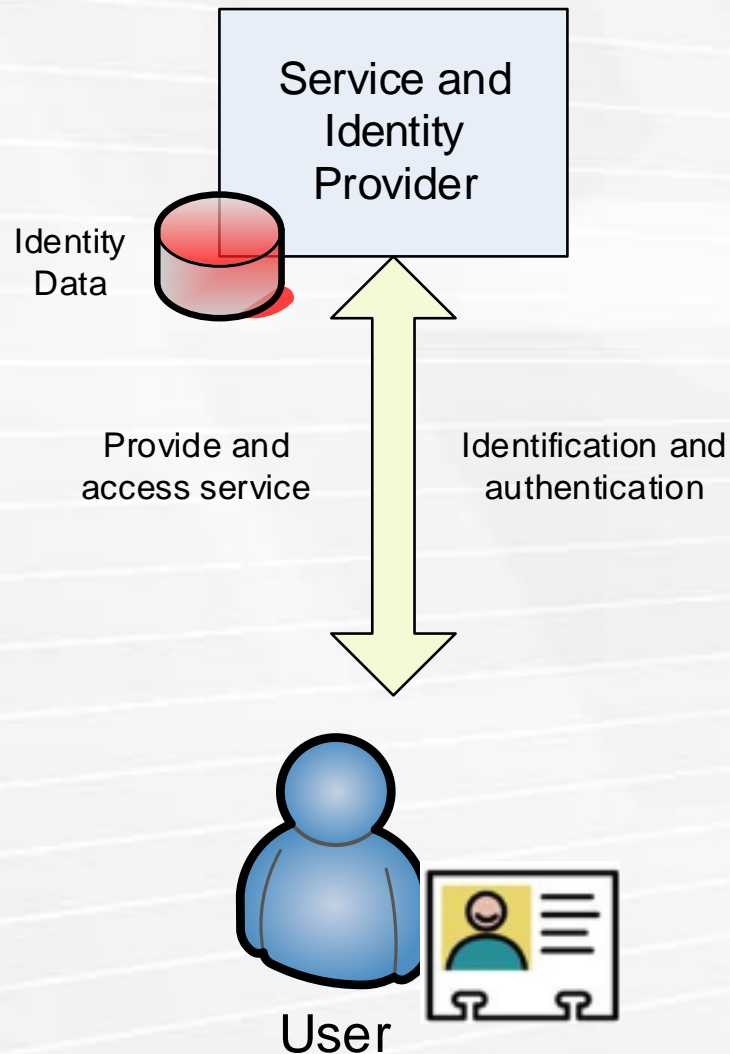
Identity Management Models | Stakeholders

- » **Subject (User)**
 - » Digital identity of a person
 - » Hands attributes to the identity provider
- » **Identity Provider (IdP)**
 - » Identification, Authentication (and Authorization)
 - » Provides subject's attributes to service provider
- » **Relying Party (Service Provider - SP)**
 - » Provides services/resources to the subject
 - » Relies on the identity data of the identity provider
 - » (Authorization)
- » **Control Party**
 - » Checks compliance of policies, guidelines or laws
 - » Contains the possibility for audit
 - » E.g.: Reproducing an authentication process



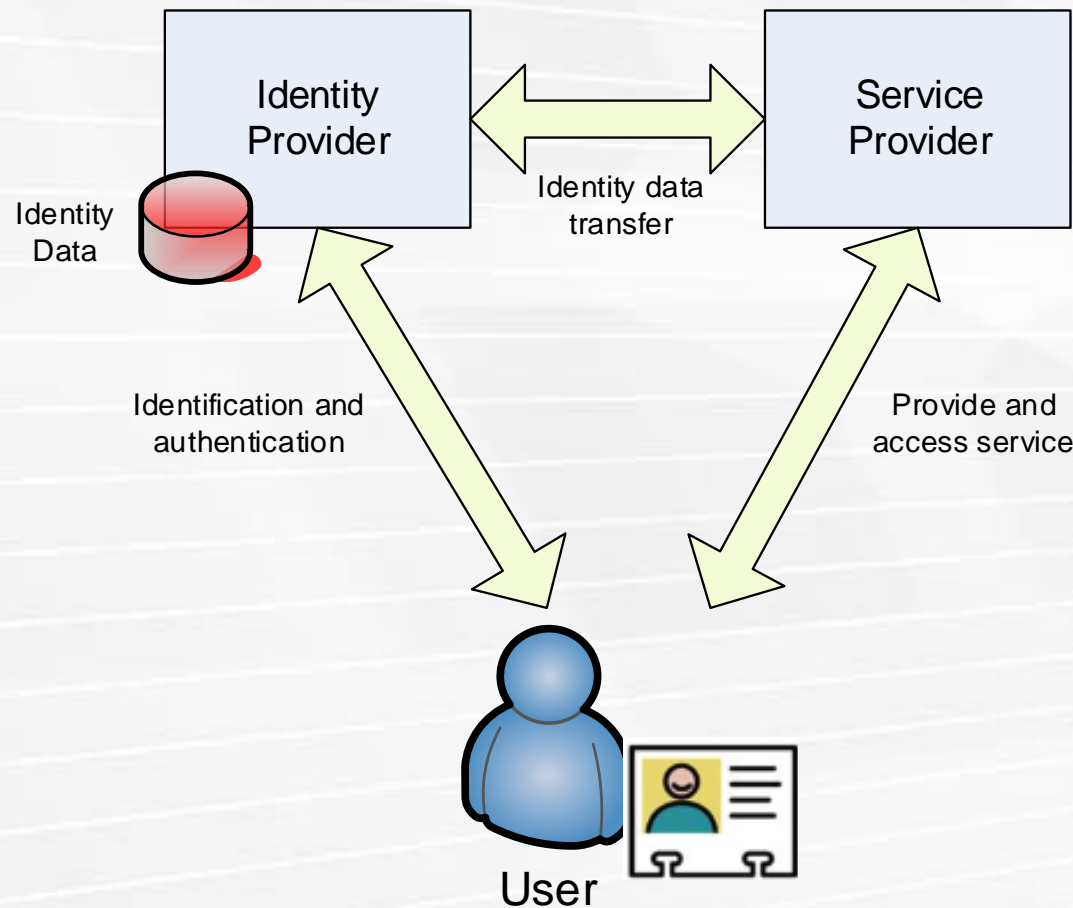
Ref: Bertino/Takahashi


Identity Management Models | Isolated Model



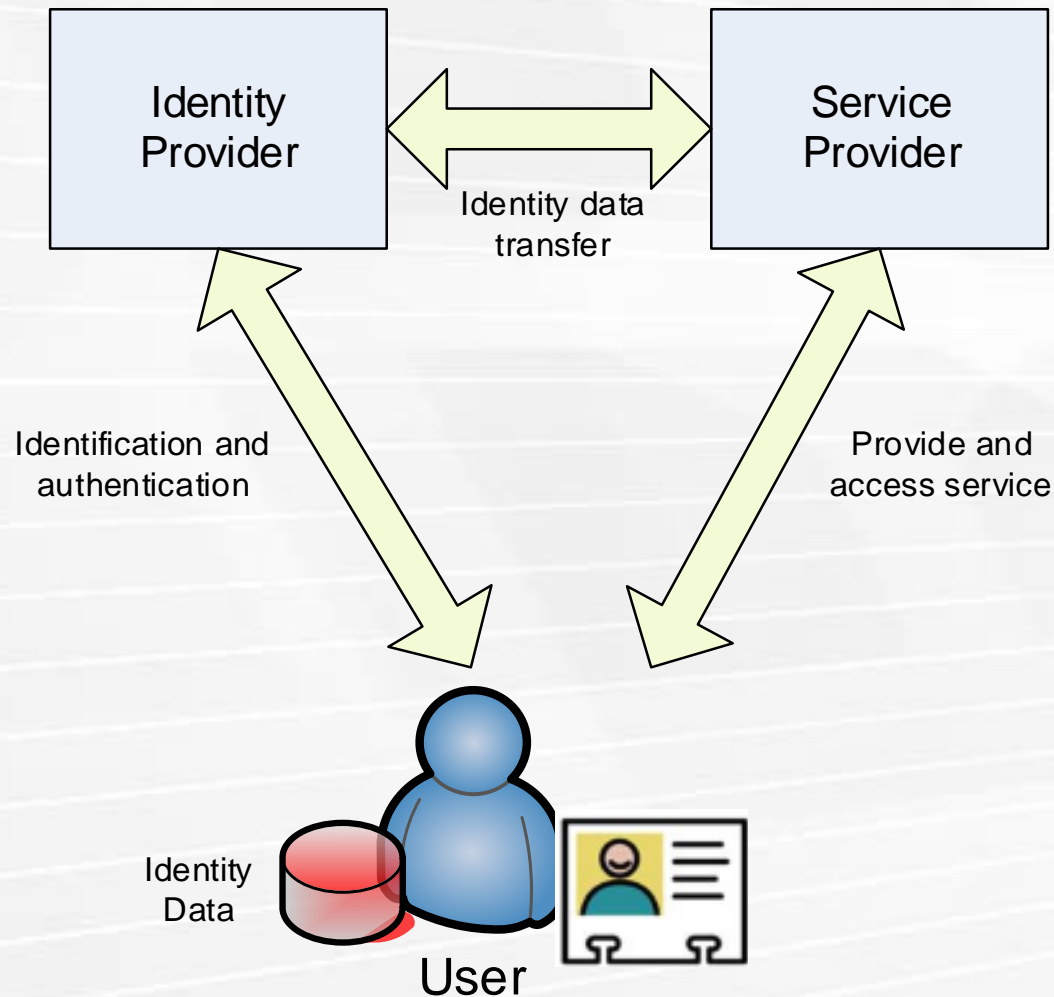
- « Service Provider is also Identity Provider
- « Authentication directly at the Service Provider
- « Identity data stored and maintained at the individual Service Provider
- « Implemented at each Service Provider individually

Identity Management Models | Central Model



- « Separation of Identity Provider (IdP) and Service Provider (SP)
- « IdP stores identity data
- « SP gets identity data from IdP
- « User: no control over actual data transfer
- « E.g.: Login with Facebook 

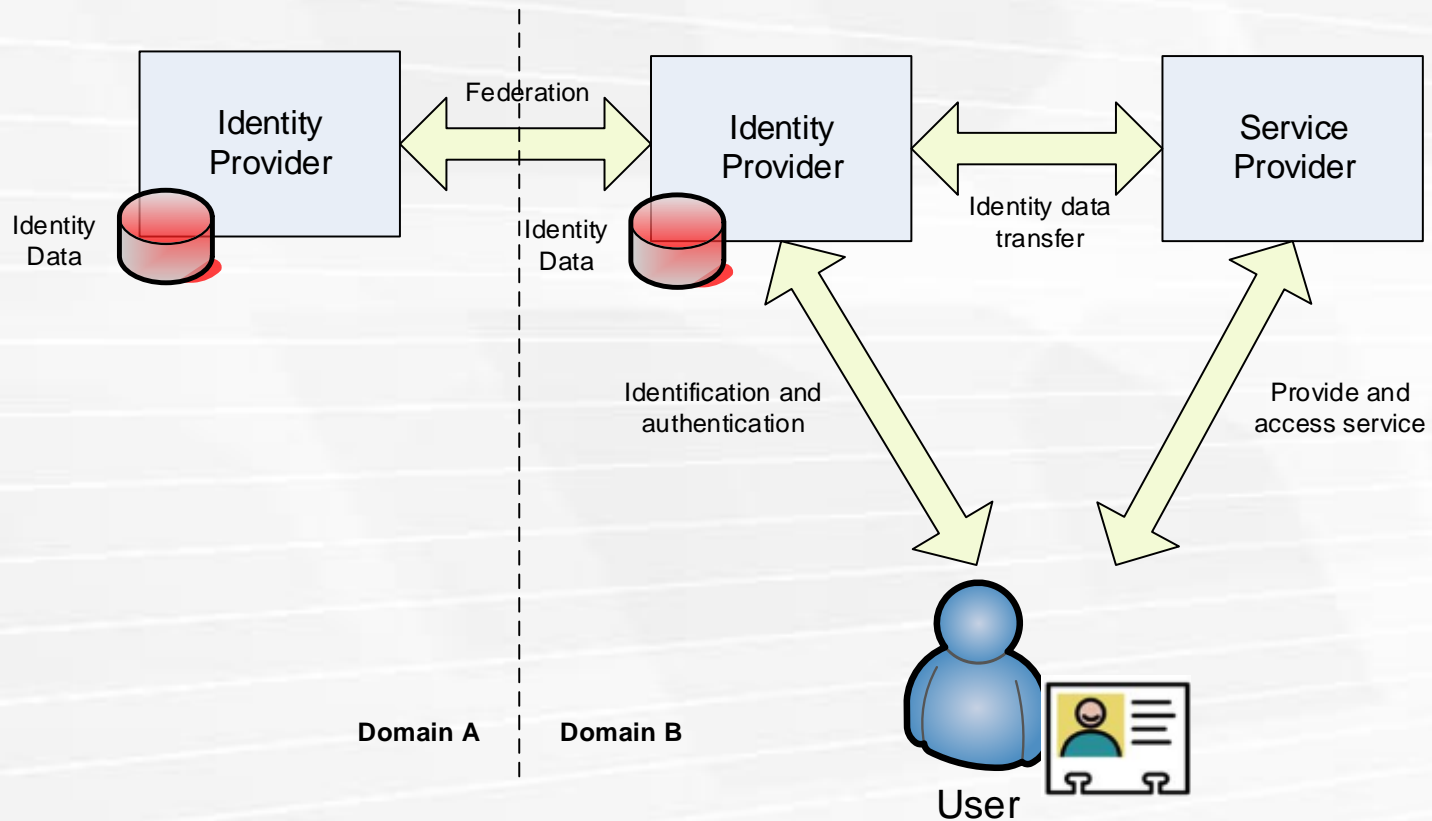
Identity Management Models | User-Centric Model



- « Identity data stored in user's domain
- « Usually on a secure token (smart card, ...)
- « Explicit user consent for sharing
- « E.g.: Austrian Citizen Card



Identity Management Models | Federated Model

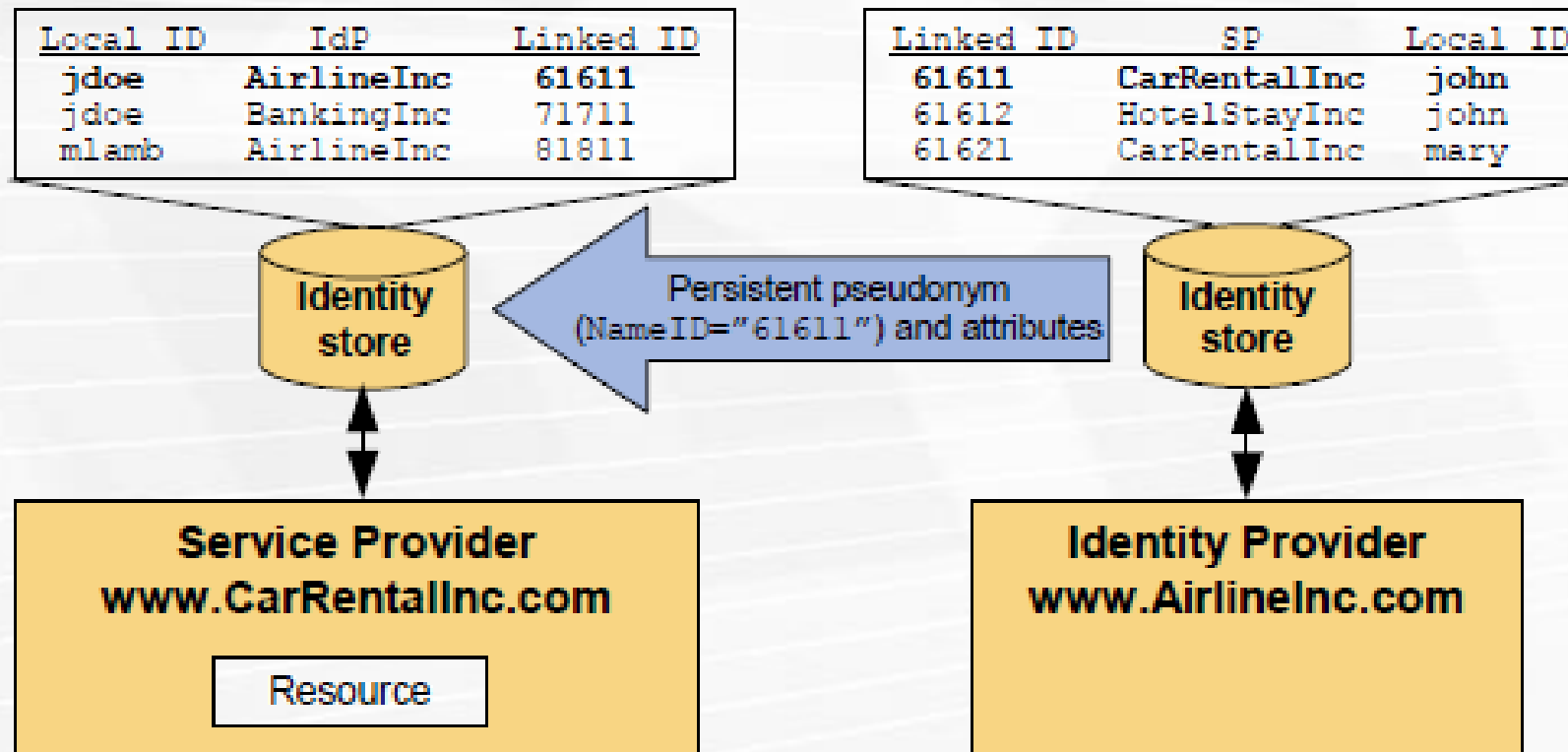


- « Identity data distributed across several IdPs
- « Data connected/compiled
 - « Trust relationship between IdPs required
 - « IdP share common identifier
- « E.g.: WS-Federation, Shibboleth



Identity Management Models | Federated Model (2)

Data Federation



Ref: SAML 2.0 Technical Overview

Identity Management | Summary

- » **Identity Management Lifecycle**
 - » Creation, Usage, Maintenance, Deletion, Governance
- » **Stakeholders**
 - » Subject, Relying Party, Identity Provider, Control Party
- » **Identity Management Models**
 - » Isolated: SP is also IdP
 - » Central: SP and IdP are separated, IdP stores user's attributes
 - » User-Centric: SP and IdP are separated, but user stores own attributes
 - » Federated: User's attributes (stored across several IdPs) and collected/combined

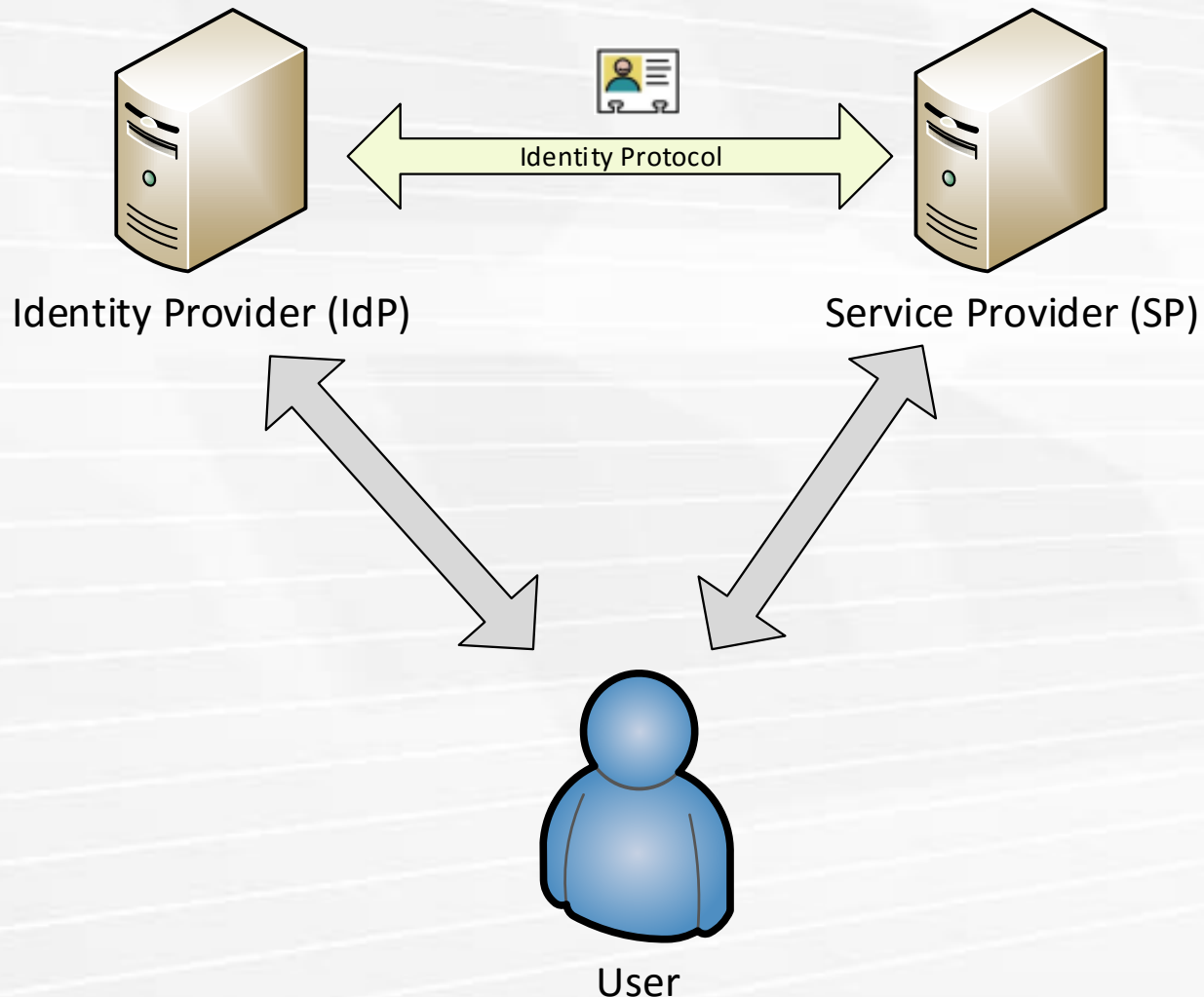
Overview

- » **General Definitions**
 - » Identity, Digital Identity, Electronic Identity
 - » Identification, Authentication, Authorization
 - » Identity Types, Threats, Challenges

- » **Identity Management**
 - » Identity Management Lifecycle
 - » Identity Management Models

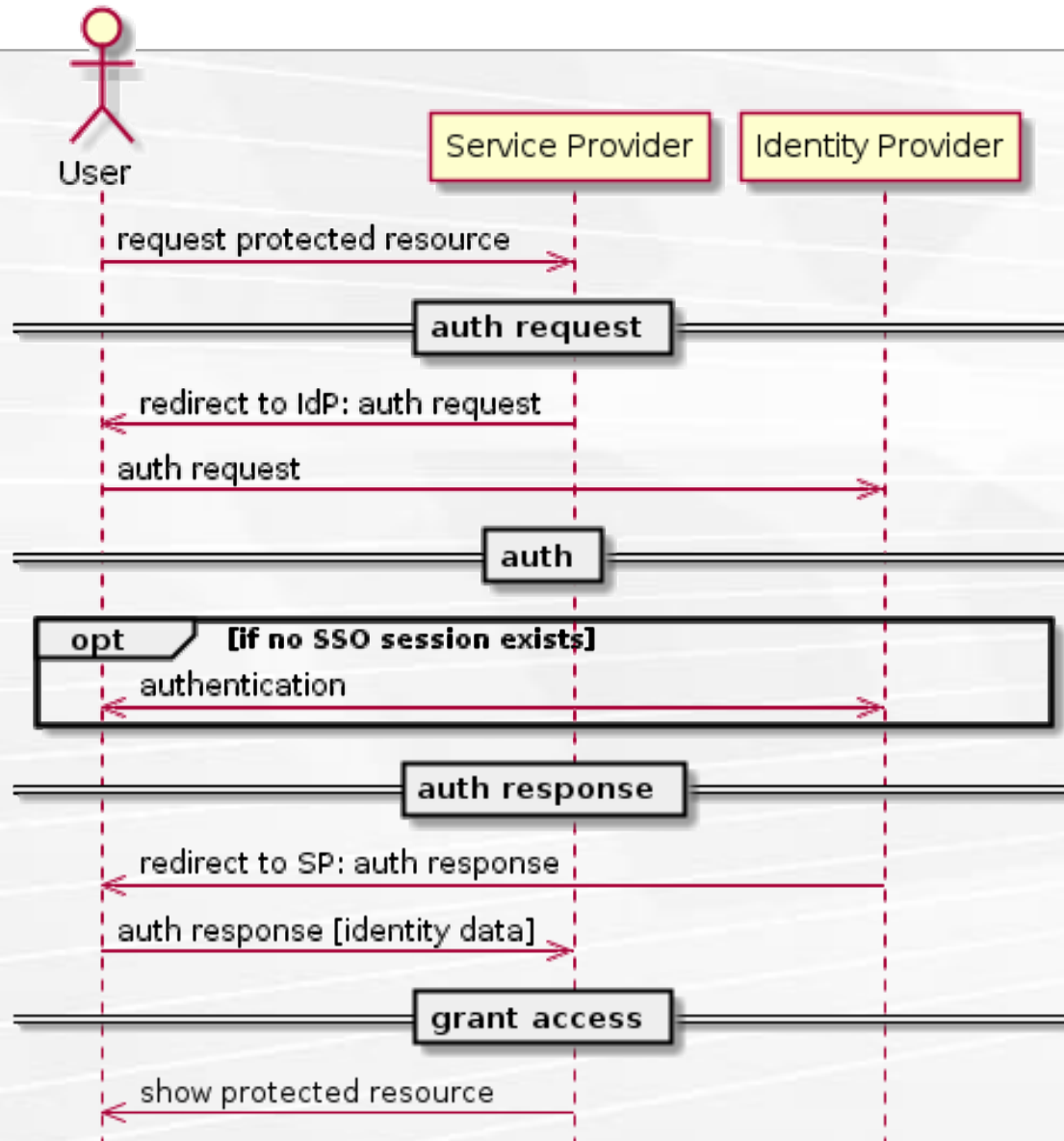
- » **Identity Protocols**
 - » SAML, OAuth, OpenID Connect

Identity Protocols



- » Identity Protocols specify communication between IdP and SP
- » Indirect communication via user
- » Used to
 - » Identify and authenticate user
 - » Exchange the user's attributes

Identity Protocols | General Process



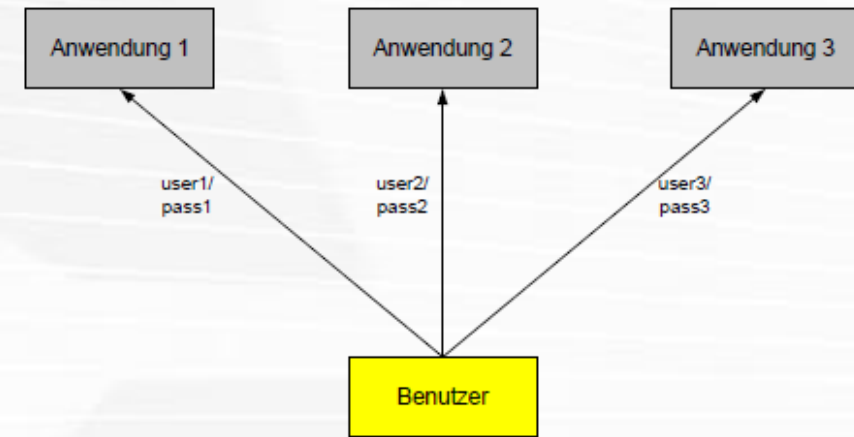
- » SP and IdP communicate indirectly
- » Redirects carries authentication request and response

1. User's agent (browser) is forwarded to IdP with auth request
2. User interacts to authenticate
3. Identity data is sent back to SP through redirect

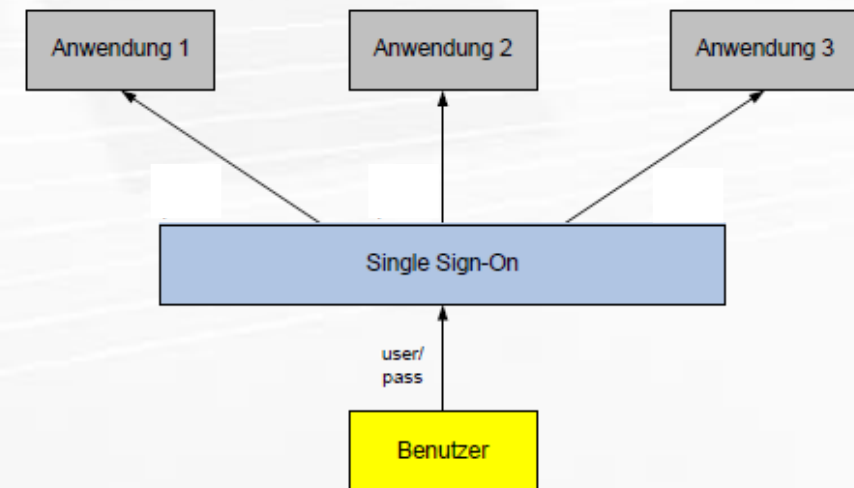
Identity Protocols | Use Cases | Single Sign-On (SSO)

SSO is the ability for a user to authenticate once to a single authentication authority and then access other protected resources without re-authenticating. [Clercq]

- » Login once - access multiple services
- » Advantages
 - » Only one authentication process
 - » Prevent large number of different passwords
 - » More user comfort and time savings
 - » Higher level of security
- » Disadvantages
 - » Central point of failure or attack



Normal login at multiple services



SSO-login at multiple services

Identity Protocols | Use-Cases (continued)

» Single Log Out (SLO)

- » Global logout at all services a user is currently logged in

» Identity federation

- » Federation of identity data across multiple systems/domains

» Attribute-based authorization

- » Authorization based on transferred attributes

» Securing Web Services

- » Transportation of structured security information within other standards

Identity Protocols | Terminology of Protocols

	SAML	OAuth	OpenID Connect
Service Provider (SP)	Service Provider (Relying Party)	Client	Relying Party
Subject	Subject	Resource Owner	End User
Identity Provider (IdP)	Identity Provider	Authorization Server AND Resource Server	Authorization Server AND Resource Server

SAML | Security Assertion Markup Language

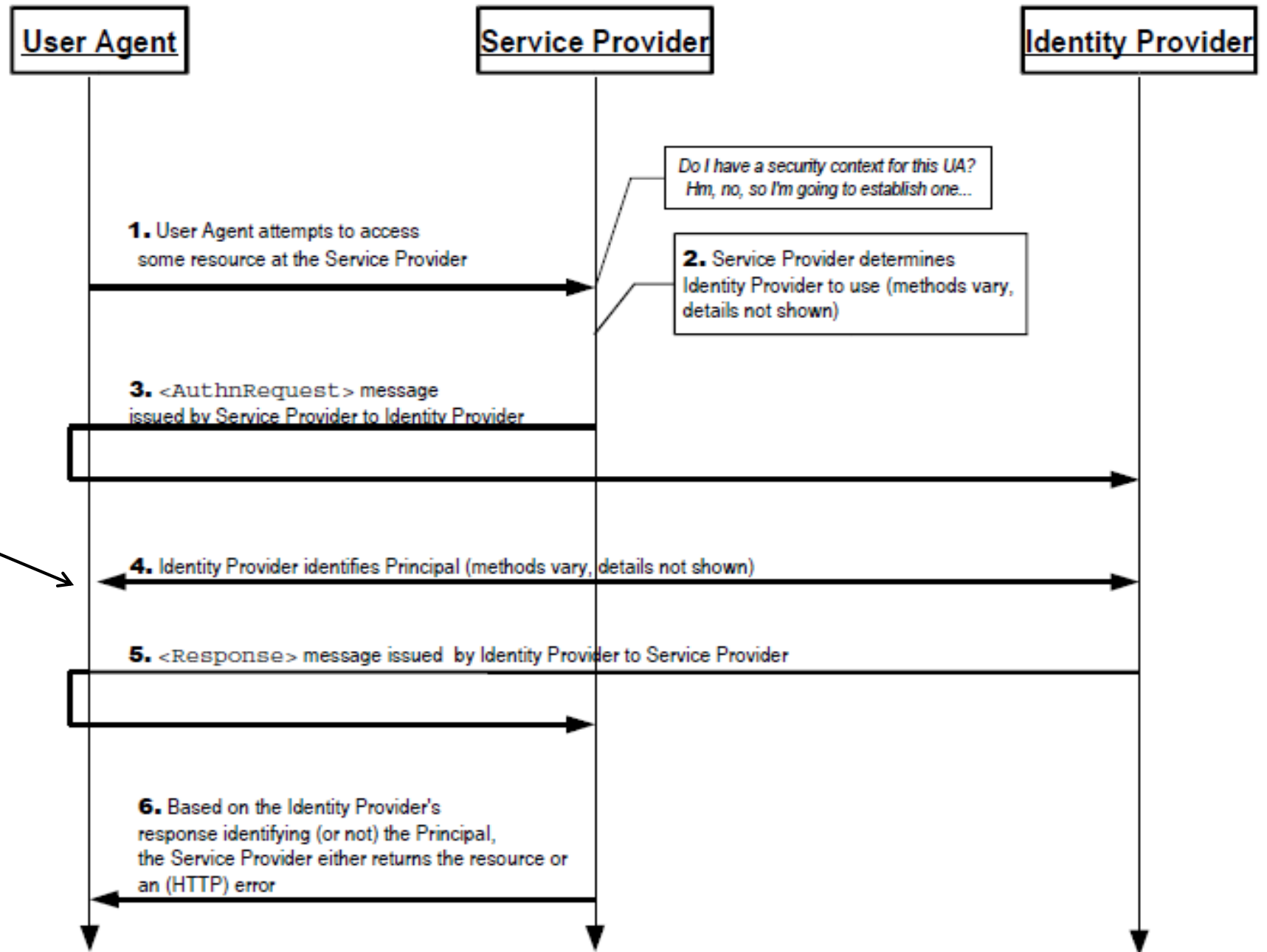
- » XML-based standard for the secure exchange of identity and authentication data between security domains
- » Well-established standard for years
 - » SAML 1.0: 2002
 - » SAML 1.1: 2003
 - » SAML 2.0: 2005
- » Uses existing standards
 - » E.g.: XML-Dsig, XML-Enc, SOAP, ...
- » Used within other standards
 - » E.g.: WS-Security



SAML | Login

» First Login

Authentication Method not specified in SAML

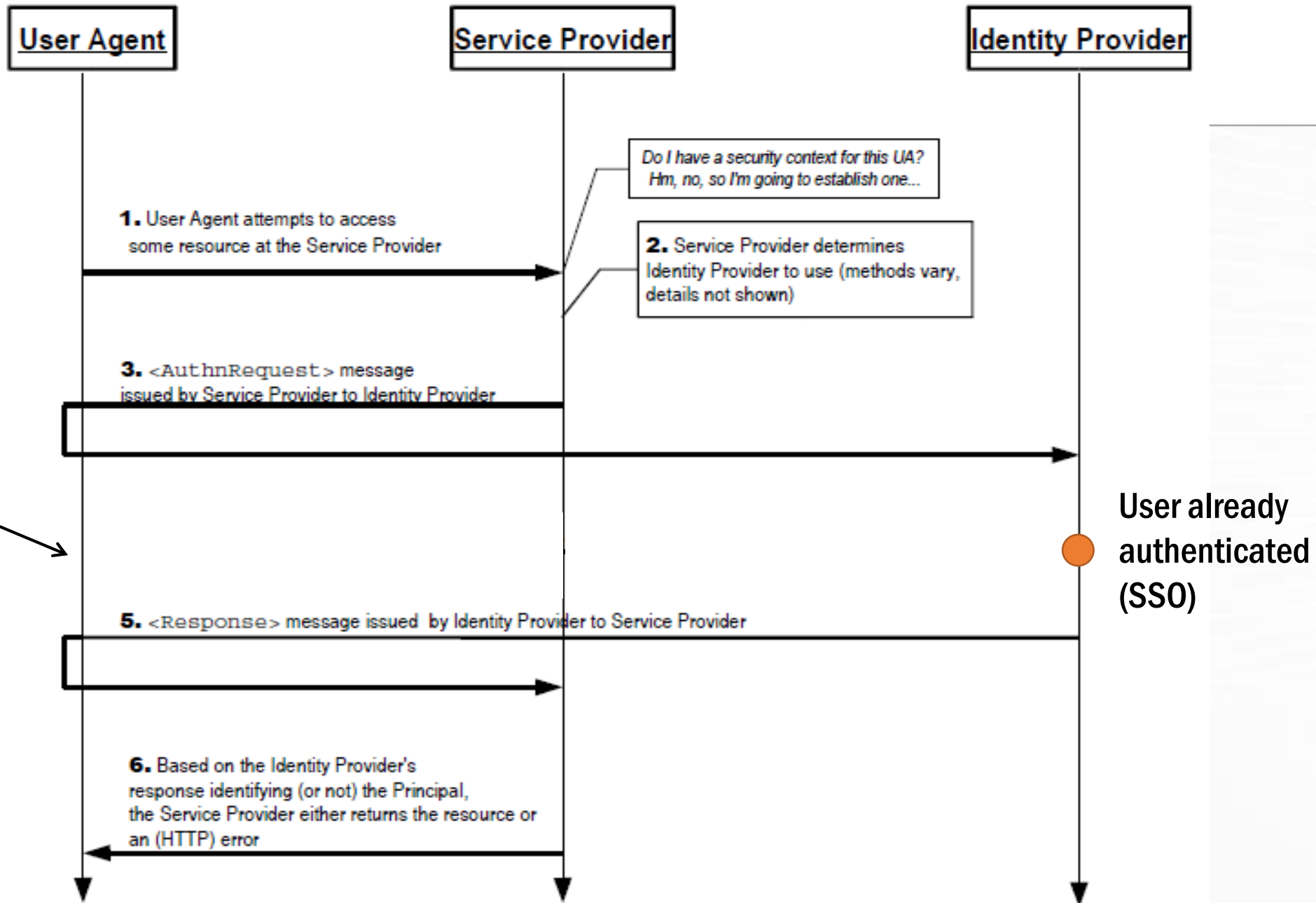


Ref: SAML 2.0 Core

SAML | Login

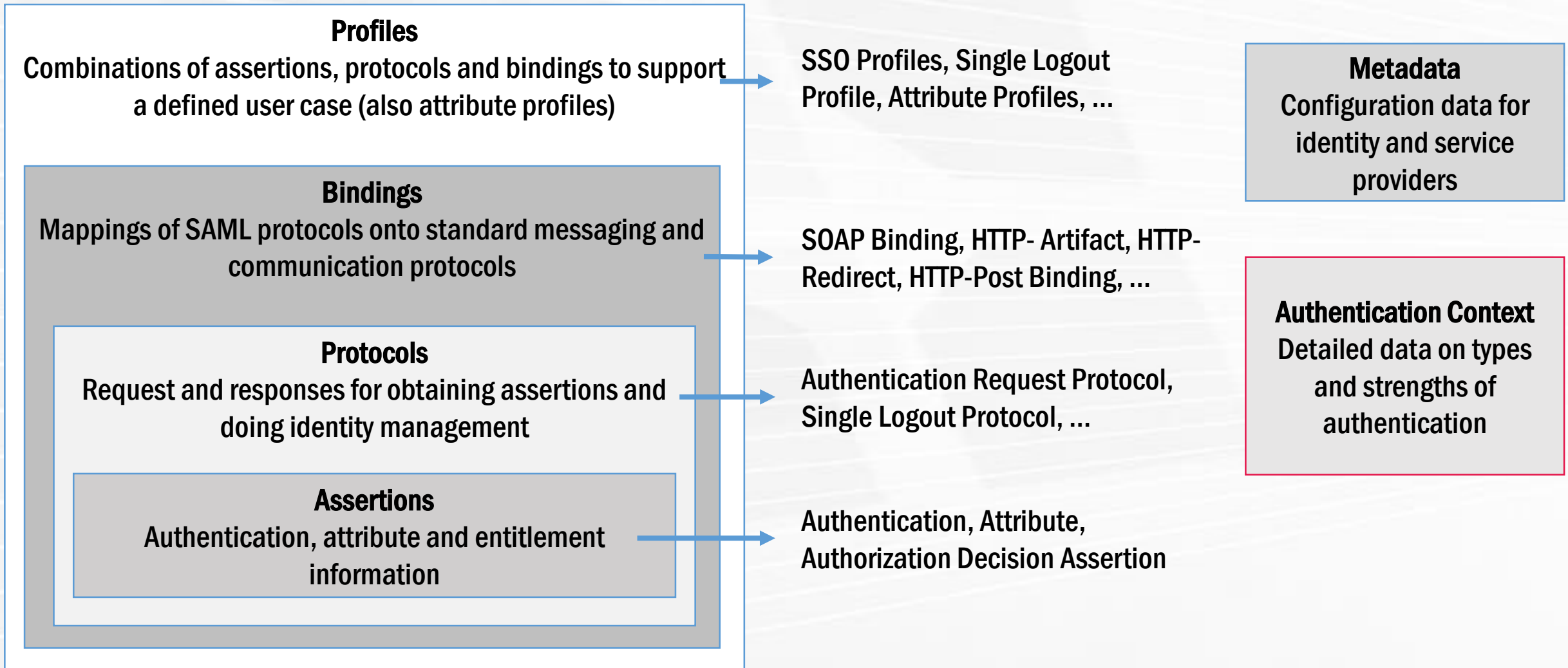
» Subsequent Login

SSO: Use existing session



Ref: SAML 2.0 Core

SAML | Architecture



Ref: SAML 2.0 Technical Overview

SAML | Assertion

» Assertion = Claim of somebody about somebody

» SAML assertions contain different statements

» Authentication statement:

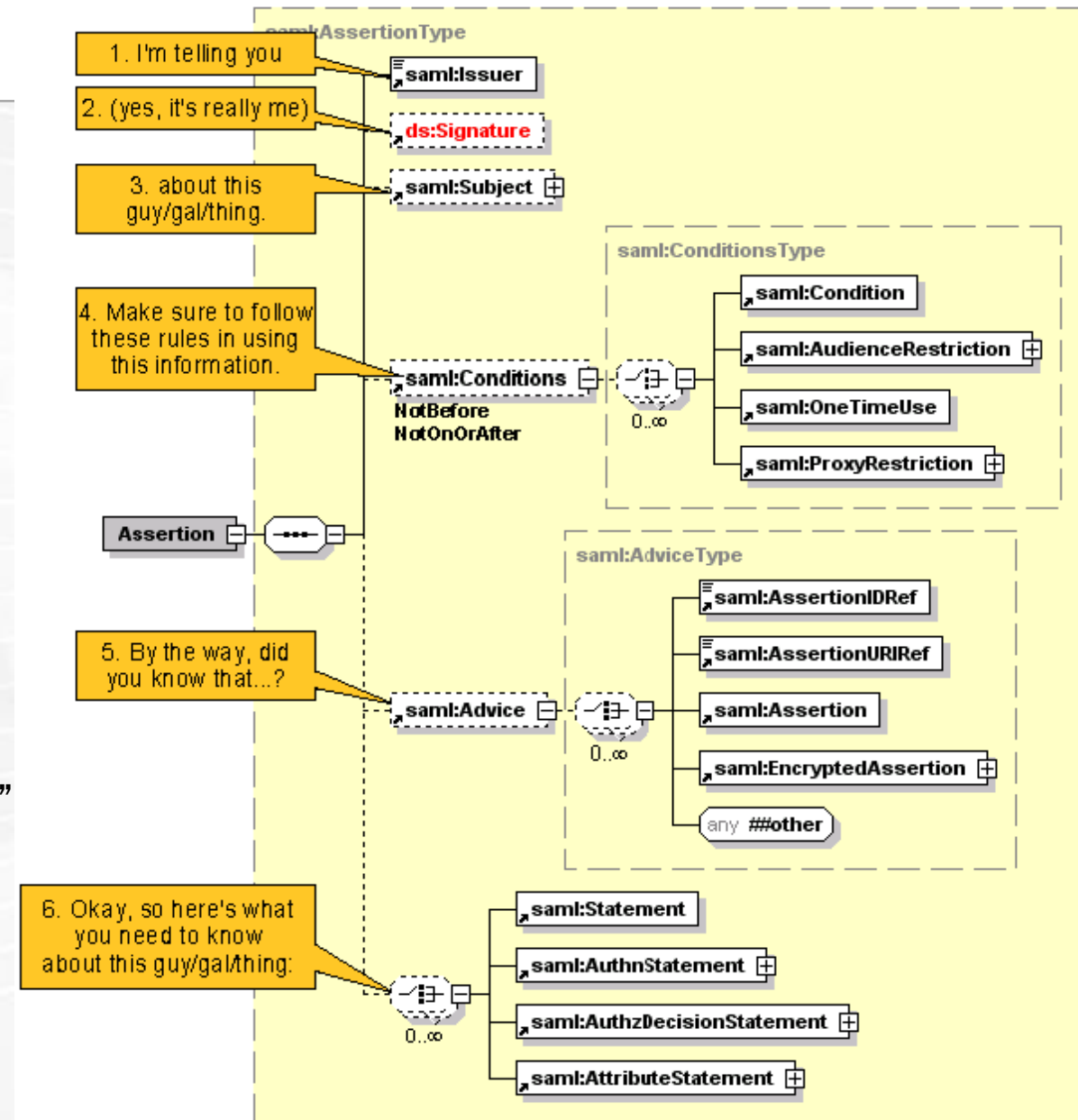
“Max Mustermann authenticated himself on October 29, 2014 at 09:17 using a smart card.”

» Attribute statement:

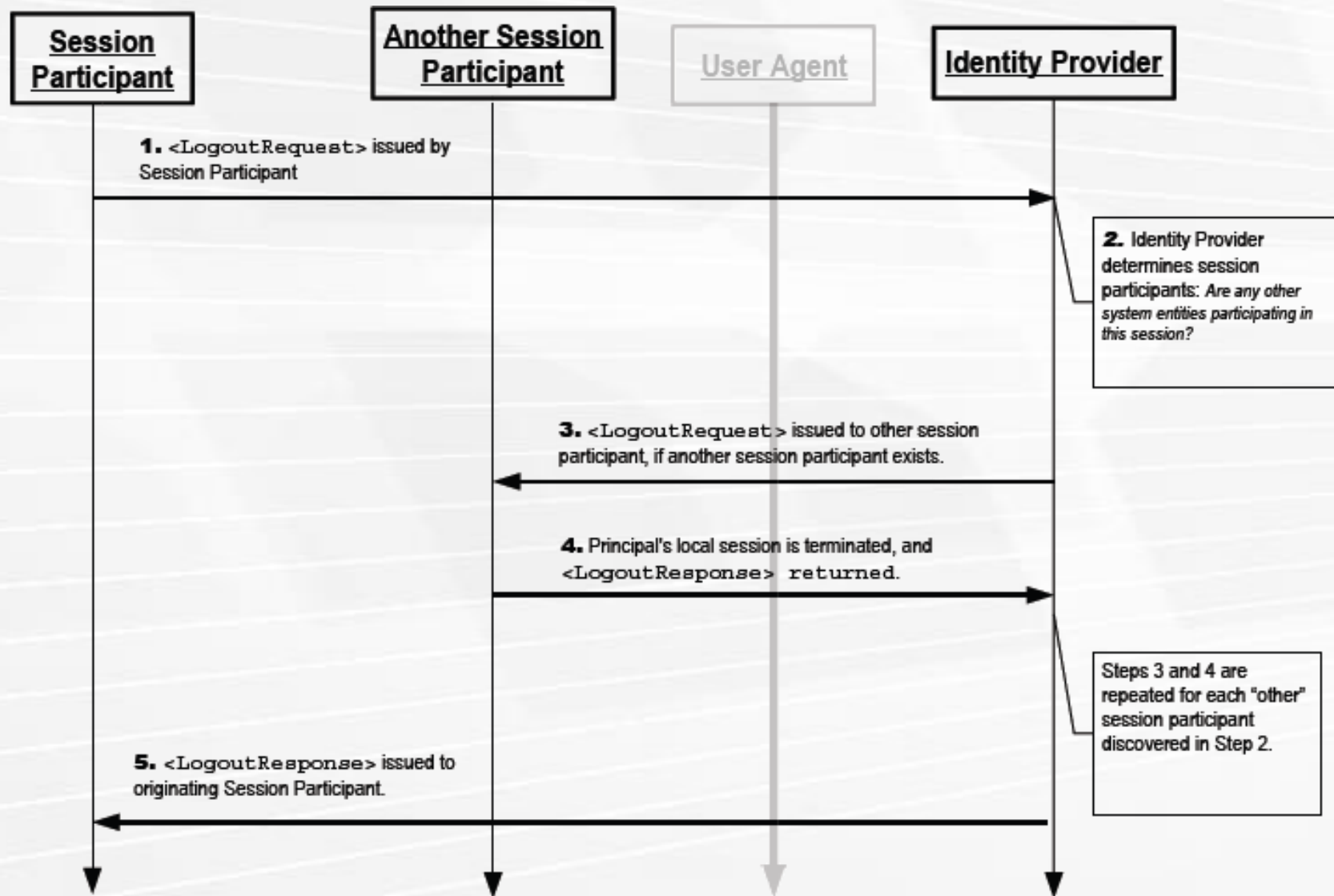
“Max Mustermann was born on January 1, 1970 and is a lawyer.”

» Authorization statement:

“Yes, Max Mustermann is allowed to access this web site”.



SAML | Single Logout



- » Upon Logout Request
- » IdP notifies all SPs
- » To terminate sessions

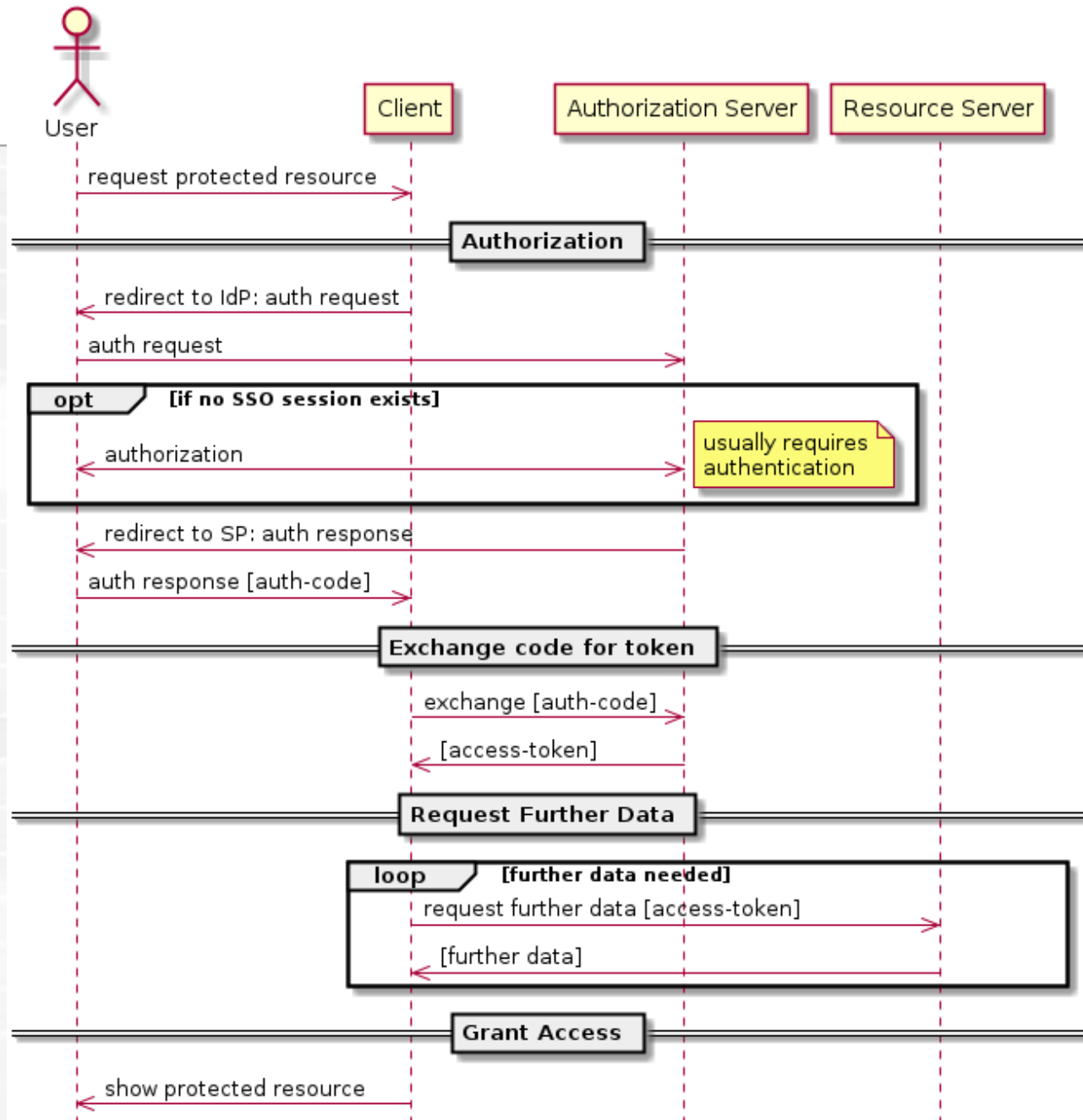
OAuth

- » Authorization protocol for desktop-, web- and mobile applications
- » Allows applications to access a user's resources
- » Users don't have to expose credentials to application
- » Established standard
 - » Version 1.0: 2010
 - » Version 2.0: 2012
- » Pseudo-Authentication
 - » Assumption: To grant access, user has to be authenticated



OAuth | Process Flow

- » Client ... Service Provider
- » Resource Owner ... User
- » Authorization Server
 - » authentication of user
 - » authorization of client
- » Resource Server
 - » hosts protected resource
- » Additionally
 - » Exchange Auth-Code for Token
 - » Get further data with token

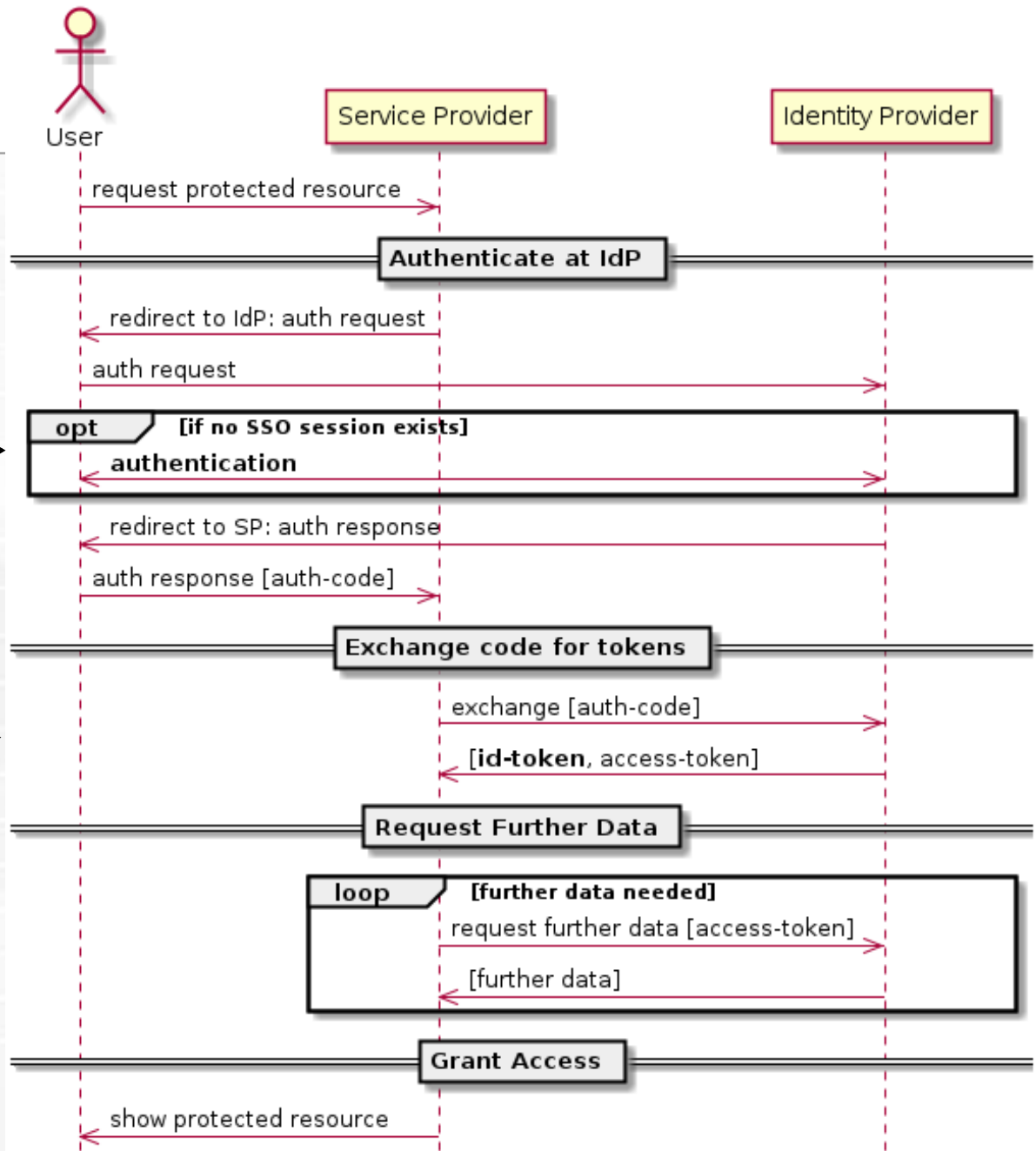


OpenID Connect

- » Identification and authentication layer based on OAuth 2.0
 - » Focus on authentication, not just authorization
 - » Support for attributes, signatures, encryption, ...
 - » Description of configuration, interoperability, ...
- » Lightweight compared to SAML
 - » No XML
 - » Only URL parameters, JSON and JWT (JSON Web Tokens)
- » Standard: Version 1.0 since 2014



OpenID Connect | Process Flow



Focus on authentication (additionally to authorization)

Already includes identity data (id-token)

OpenID Connect | Comparison to SAML

» Authentication Request & Response

OpenID Connect

```
https://moa-id.gv.at/authorize
?response_type=code
&client_id=s6BhdRkqt3
&redirect_uri=https%3A%2F%online.applikation.gv.at%2Fcb
&scope=openid%20profile
&state=af0ifjsldkj
```

```
HTTP/1.1 302 Found
Location: https://online.applikation.gv.at/cb
?code=Sp1xl0BeZQYbYS6WxSbIA
&state=af0ifjsldkj
```

» Authentication Request

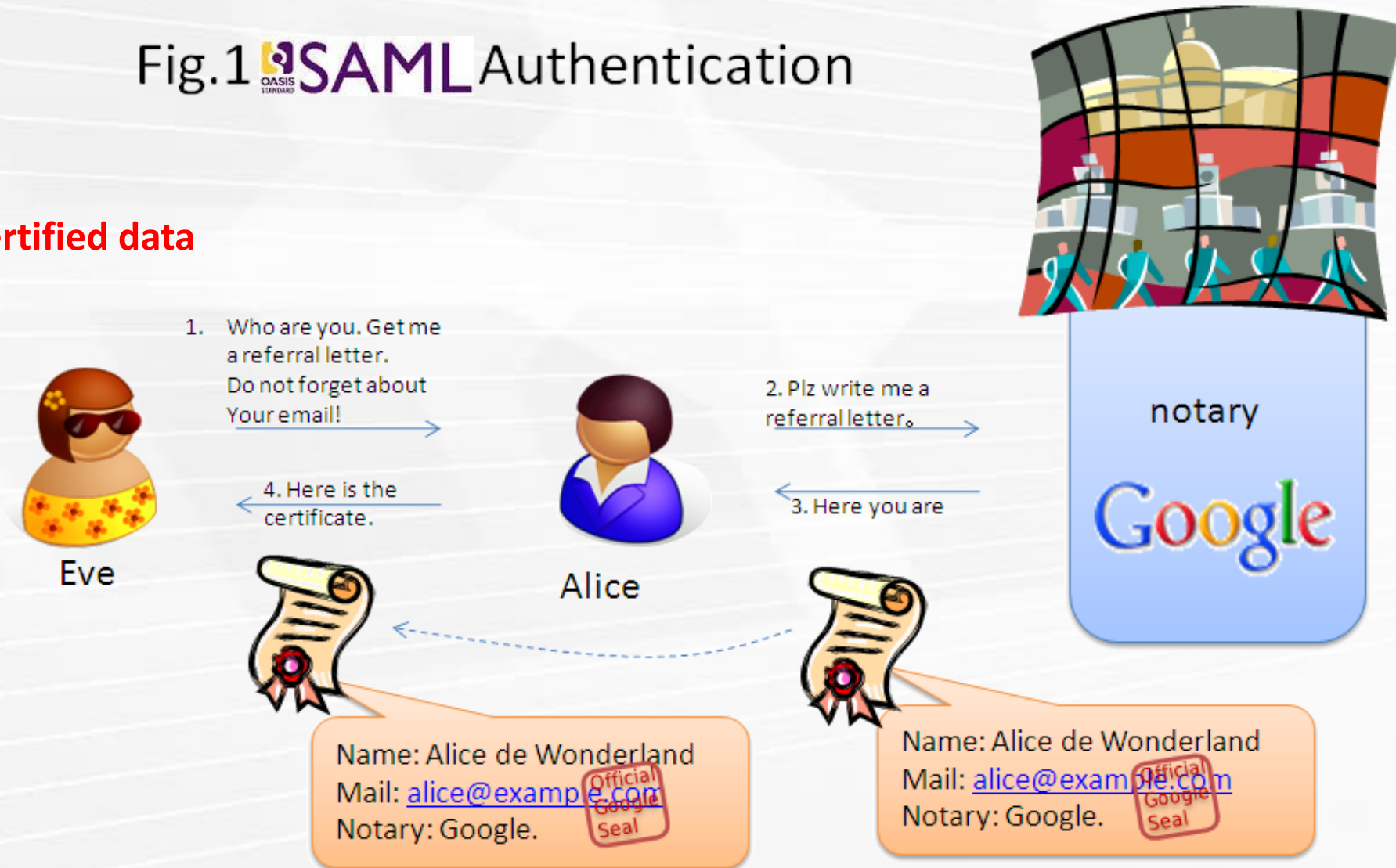
SAML

```
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
AssertionConsumerServiceIndex="1" AttributeConsumingServiceIndex="0"
Destination="https://demo.ebiz.gv.at/demportal_moaid-2.0/pvp2/post"
ID="_e1ecdd2d80062991f8f0489dfc49441" IssueInstant="2013-08-13T14:13:29.392Z" Version="2.0">
<saml2:issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">demologin-pvp2-ss0/main/</saml2:issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
<ds:Reference URI="#_e1ecdd2d80062991f8f0489dfc49441">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
<ds:DigestValue>qGqKR6stEnKFS04DQ6yx44CDzoz=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>GhvpD+urP2BwEaejBW3Y3dmdIKdFR9AikVn0TAyWBg3d/+gYxBQQUJHPn/XCoHP6QQHbNHjfq8o2wJqX9WD/BPJHK2wweczPK2cClco5bGqHq+LkwhPeshu10nrfj4T8IAHX4PIYR50EDMXV15vHWzXEBGh/MyJtk2q
AFDT40flineNk8hYpJcwN8MwMME+tiR97snFMzKl5HsKB8LzGIPq+K2A0c06AX2LIT8xaDscJTqqeaz4zlm6haZ1LZX0qMH2fJIVJAYvV2BhdSs6aseTlSp+k2ifJqvpds8PBN26I8KYb/bwQZ0hSSo//+q2cw==</ds:SignatureValue>
<ds:KeyInfo>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>nEPzKMh3TovnfBnTy+TMYFSGep8UI7iNbnYfLoBfqRdeGDok4es2qWkgB6az+km/9Js2H06m4
pjE7/RljD0IMWagi8eqdJlMmbFQykyYQhZbwi8KqBcCKj5N3G4qh8A5qN4y85Q3sZ23T
iilY1rpe+ZTOHCm6CkeRso9j409YHP1xAXFPvly2TA1uuagxOml750C/hr7gcUm0tmuKISeg
+T04Vzw2Q7K7YESZ1WkiBoG2I4cHdcBFKvRvGNtyl6UkVWXRJSU9aNL5QxsE6iFwCvFoIU
cWxIFHq0GbrAcRUB4fk+KFHE2o1DLmfWZaUQ==</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
</ds:Signature>
<saml2:Subject xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:NameID>demologin-pvp2-ss0/main/</saml2:NameID>
</saml2:Subject>
<saml2p:NameIDPolicy AllowCreate="true"
Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" />
<saml2p:RequestedAuthnContext>
<saml2:AuthnContextClassRef comparison="minimum" xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">http://www.stork.gov.eu/1.0/citizenQAALevel/4</saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```


Identity Protocols | Differences Summary

Fig.1  SAML Authentication

SAML:
SP gets **certified data**



Identity Protocols | Differences Summary

Fig.2 Pseudo-Authentication using OAuth

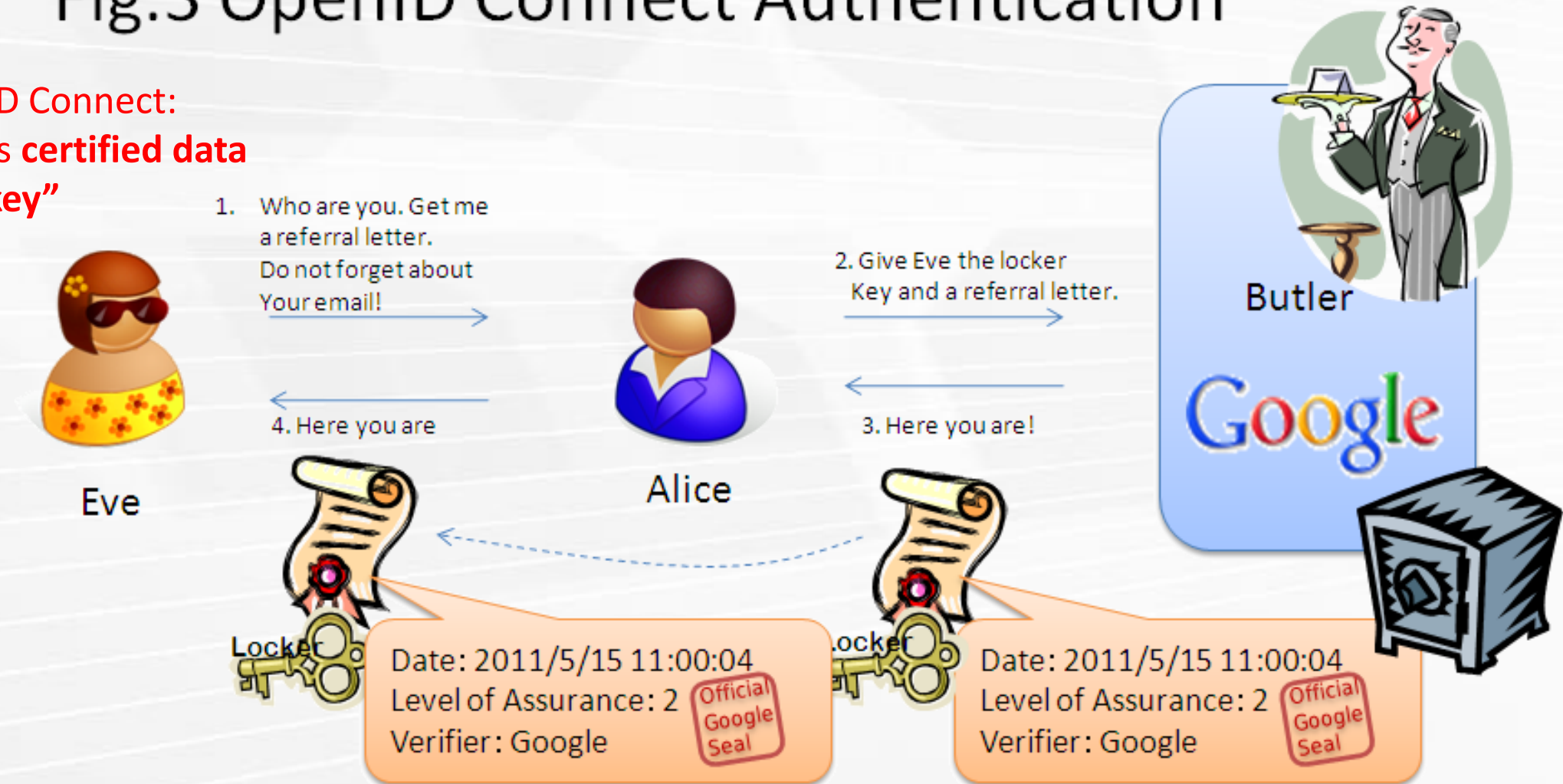
OAuth:
SP gets "key"



Identity Protocols | Differences Summary

Fig.3 OpenID Connect Authentication

OpenID Connect:
SP gets **certified data**
and **“key”**



Identity Protocols | Summary

- » **General Process:**
 1. SP forwards user with authentication request to IdP
 2. IdP authenticates user and obtains authorization
 3. IdP sends user back to SP with requested data
- » **Single Sign-On: log in once – access many services**
- » **Single Logout: log out of all services with one click**

- » **SAML: SP gets certified data**
- » **OAuth: SP gets “key” to access data**
- » **OpenID Connect: SP gets certified data and “key” to access**

Identity Management

Felix Hörandner

felix.hoerandner@iaik.tugraz.at

www.egiz.gv.at



EGIZ

E-Government Innovationszentrum

References

- » E-Government Law: <http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230>
- » L. J. Camp : Digital Identity. In: *Technology and Society Magazine*, 2004, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1337889>
- » R. Clarke: “Human identification in Information Systems: Management Challenges and Public Policy Issues”, *Information Technology & People*, 1994, Vol. 7, pp. 6-37, <http://www.rogerclarke.com/DV/HumanID.html>
- » E. Bertino, K. Takahashi: “Identity Management: Concepts, Technologies, and Systems”, 2011
- » A. Tsoikas, K. Schmidt: „Rollen und Berechtigungskonzepte“, 2010
- » J. Palfrey, U. Gasser: „Digital Identity Interoperability and Innovation“, 2007
- » J. D. Clercq: “Single Sign-On Architectures”, *InfraSec 2002*, pp. 40-58
- » SAML: <http://saml.xml.org>
- » OAuth: <http://oauth.net>
- » OpenID Connect: <http://openid.net/connect/>
- » N. Sakimura: „Dummy’s guide for the Difference between OAuth Authentication and OpenID“, 2011, <http://nat.sakimura.org/2011/05/15/dummys-guide-for-the-difference-between-oauth-authentication-and-openid/>
- » Fidis: <http://www.fidis.net>
- » GINI-SA: <http://www.gini-sa.eu>

Identity Management | Control Questions

- » Explain the terms identification, authentication, and authorization. Give one example for means of identification and one for authentication mechanisms.
- » What is multi-factor-authentication? Give an example.
- » Explain the identity lifecycle, including its stages.
- » What is a digital identity? What are its 3 parts? What is the difference to an electronic identity? Explain the level of assurance.
- » Explain 4 (of 8) identity types, 2 (of 4) challenges, and 3 (of 6) threats.
- » Enumerate and explain the stakeholders that are involved within an identity management system.
- » Describe the 4 identity management models.
- » Enumerate the identity protocols. Describe one of them in detail, including protocol steps.