Federated identity management, STORK, eIDAS

Herbert Leitold

COINS summer school on authentication
Metochi, Lesbos, August 1st - 2nd, 2016

Introducing myself …

- Professional background
  - 1995-2002: Research Assistant at Graz University of Technology
    - Main research area: Network security
  - Since 2003: Director of Stiftung SIC
    - Non profit foundation on information sec.
  - Since 2002: A-SIT
    - Electronic signatures, eID
- Some projects and duties
  - STORK: 2008-2015
  - eIDAS Expert Group and Tech. Subgr.

Introducing the lecture …

- The elevator pitch on identity federation:
- Ingredients
  - Take what you might already know …

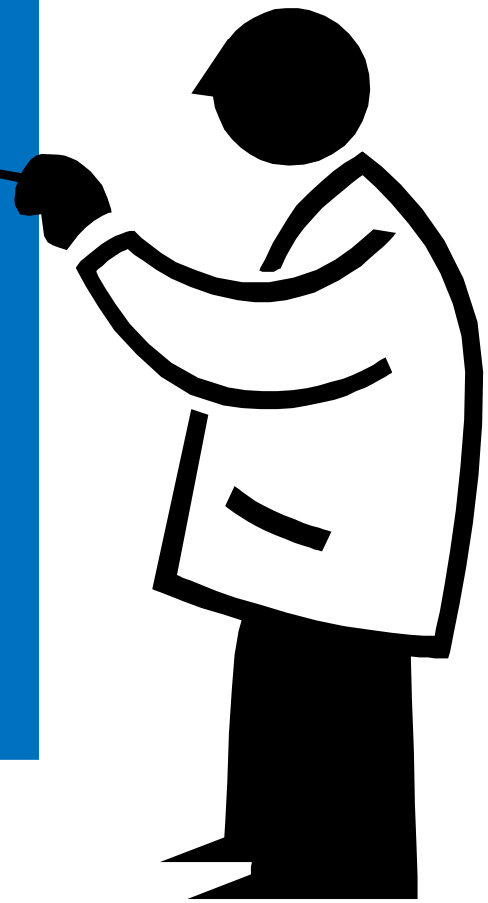
ID-porten

  - try adding heterogeneity and complexity of
    - 28 EU Member States plus EEA
    - many sectors, more Identity Providers, and countless services

… and its technical/organisational/policy challenges

Contents

- Motivation, Terminology
- Federation Protocols
- STORK and STORK 2.0
- eIDAS



SECTION 1:

ID - what if something goes wrong

Example for Identity Theft

Mat Honan

In the space of one hour, my entire digital life was destroyed. First my Google account was taken over, then deleted. Next my Twitter account was compromised, and used as a platform to broadcast racist and homophobic messages. And worst of all, my AppleID account was broken into, and my hackers used it to remotely erase all of the data on my iPhone, iPad, and MacBook.

In many ways, this was all my fault. My accounts were daisy-chained together. Getting into Amazon let my hackers get into my Apple ID account, which helped them get into Gmail, which gave them access to Twitter. Had I used two-factor authentication for my Google account, it's possible that none of this would have happened, because their ultimate goal was always to take over my Twitter account and wreak havoc. Lulz.

http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/

Government eID projects …

Early birds started late 1990's early 2000

– Finish eID card: December 1999

– Estonian eID card: from January 2002

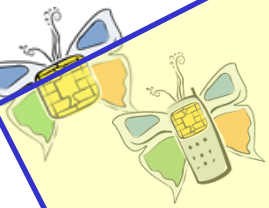
– Austrian citizen card: from 2003, mass-rollouts 2005

– Italian CIE / CNS: test phase 2003 (CIE)

– Belgian eID card: from 2nd half 2003

Government eID projects …

Early birds started late 1990's early 2000



– Finish eID card: December 1999

– Estonian eID card: from January 2002

– Austrian citizen card: from 2003, mass-rollouts 2005

– Italian CIE / CNS: test phase 2003 (CIE)

– Belgian eID card: from 2nd half 2003

Evolved as national islands

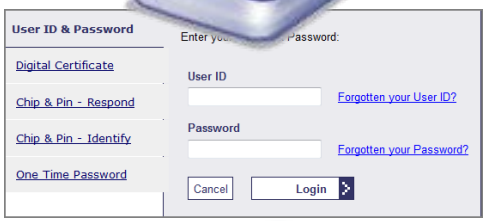
Starting Point: National eIDs

- Heterogeneous in various dimensions
  - Technology
    - Smartcards: AT, BE, DE, EE, ES, FI, IT, PT, SE, …..
    - Mobile eID: AT, EE, FI, LU, NL, NO, UK, …
    - Soft certif.: ES, SE, SI, …
    - usern./pass.: NL, UK, …

    … STORK operated on some 100+ tokens
  - Operational
    - Issued by public sector, private sector, combined
    - Issued at federal, local, regional level
    - Use of identifiers
  - Legal
    - (limited) use of identifiers; flat, sectoral, combined
    - (lacking) mutual recognition

Starting Point: National eIDs

- Heterogeneous in various dimensions
  - Technology
    - Smartcards: AT, BE, DE, EE, ES, FI, IT, PT, SE, …..
    - Mobile eID: AT, EE, FI, LU, NL, NO, UK, …
    - [illegible]: ES, SE, SI, …
    - [illegible]: NL, UK, …
    - STORK operates with some 100+ tokens
  - Organisational
    - Issued by public sector, private sector, combined
    - Issued at federal, regional level
    - Use of identifiers
  - Legal
    - (limited) use of identifiers; flat, sectoral, combined
    - (lacking) mutual recognition



Claim 2: None is the "better" system, they're just different

Cross-border cases

- A few examples …
  - Student mobility
  - Migrant workers
  - Social security
  - E-Health
  - Services Directive
  - Moving house …

  … and many, many more private sector applications!

Need of cross-border citizen services?

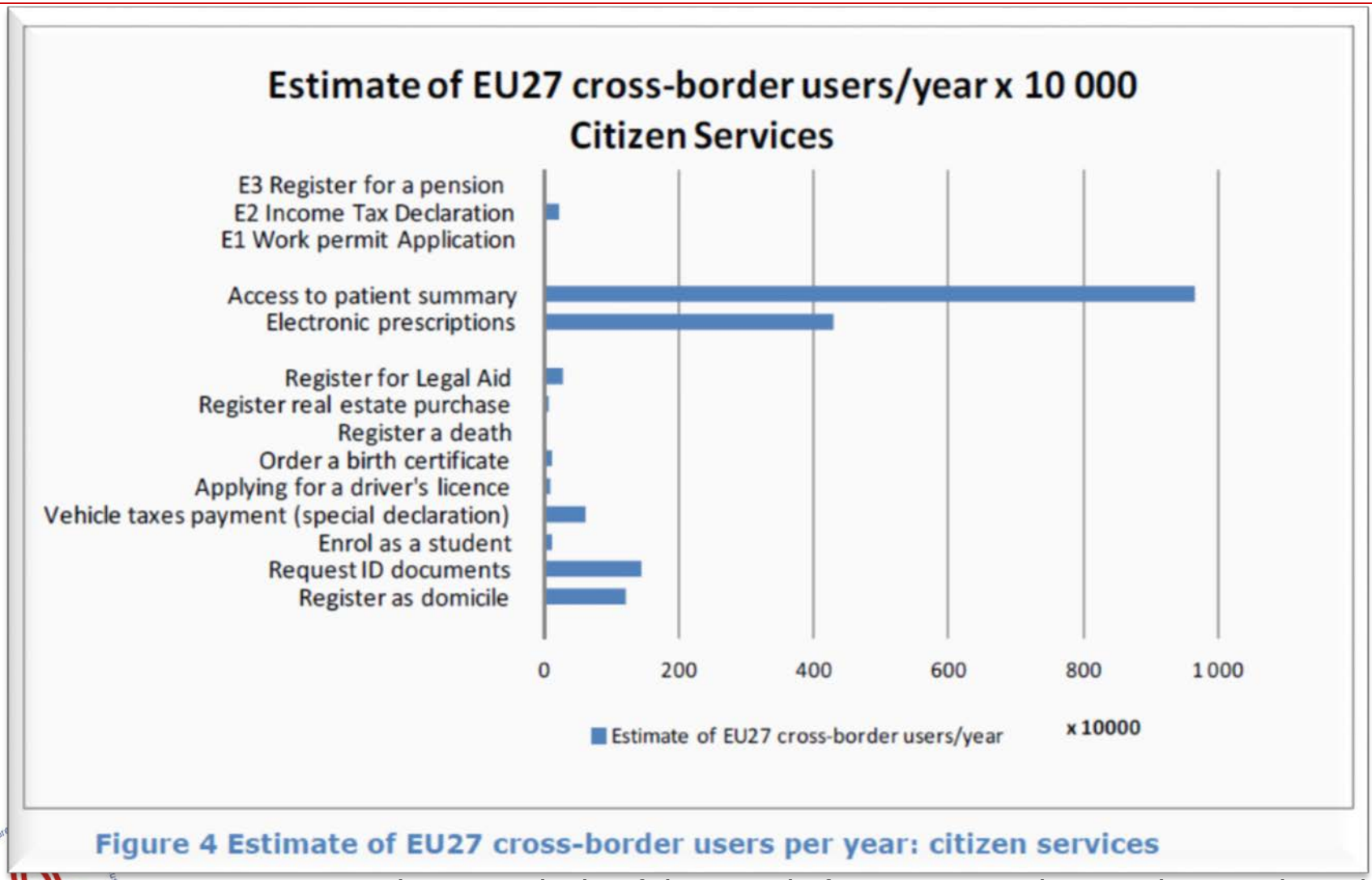


Figure 4 Estimate of EU27 cross-border users per year: citizen services

Source: EC Study on Analysis of the Needs for Cross-Border Services … (2013)

Need of cross-border business services?

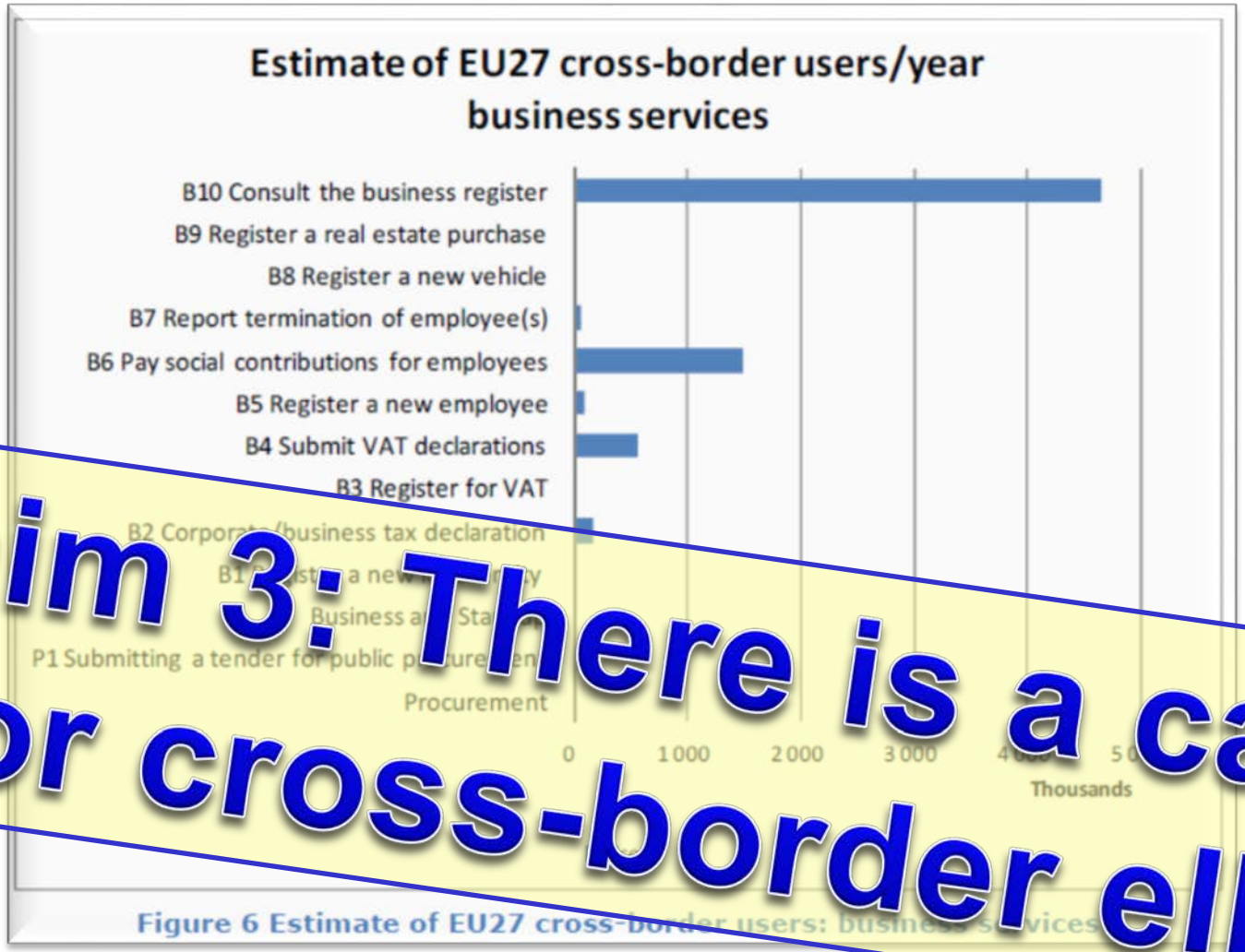


Figure 6 Estimate of EU27 cross-border users: business services

Claim 3: There is a case for cross-border eID

Source: EC Study on Analysis of the Needs for Cross-Border Services … (2013)

A little history: Manchester Ministerial Declaration

(November 2005)

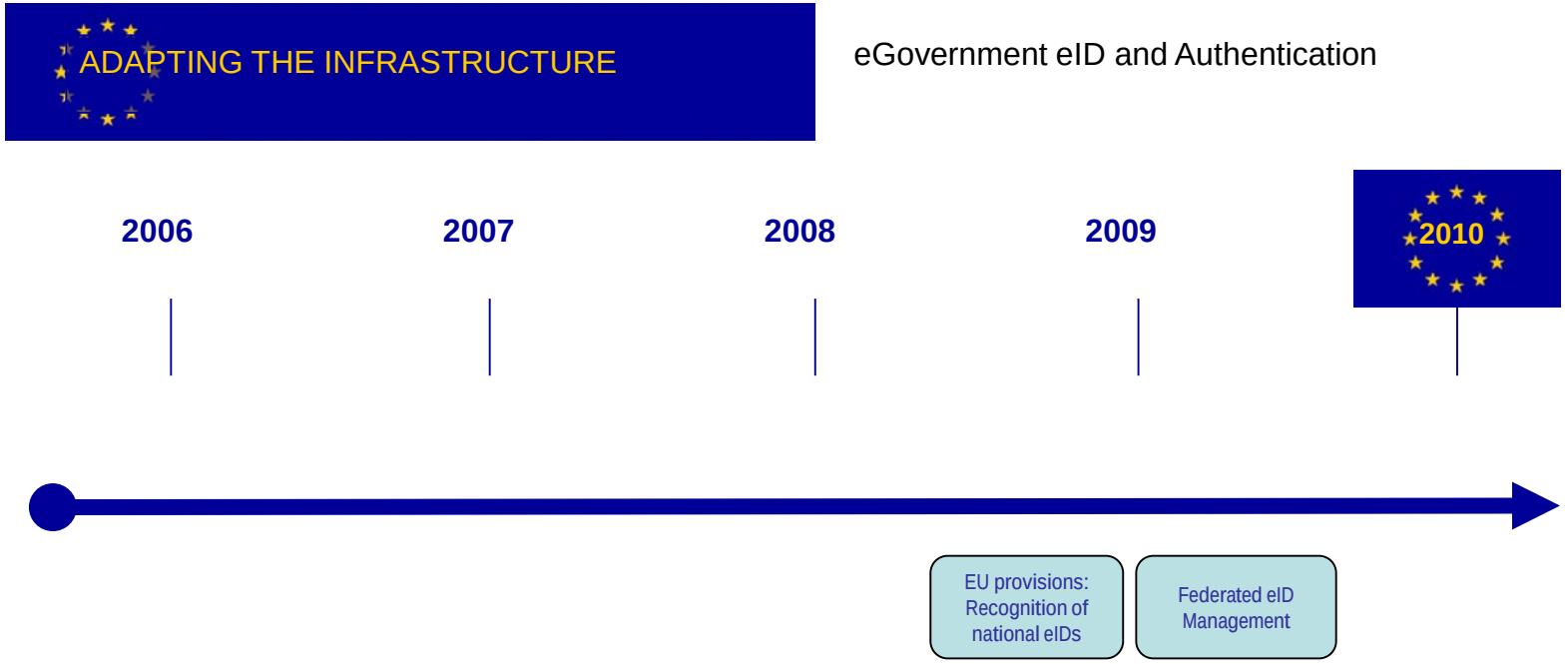
By 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations.

Such means shall be made available under the responsibility of the Member States but recognised across the EU

A little history: eID ad hoc-group

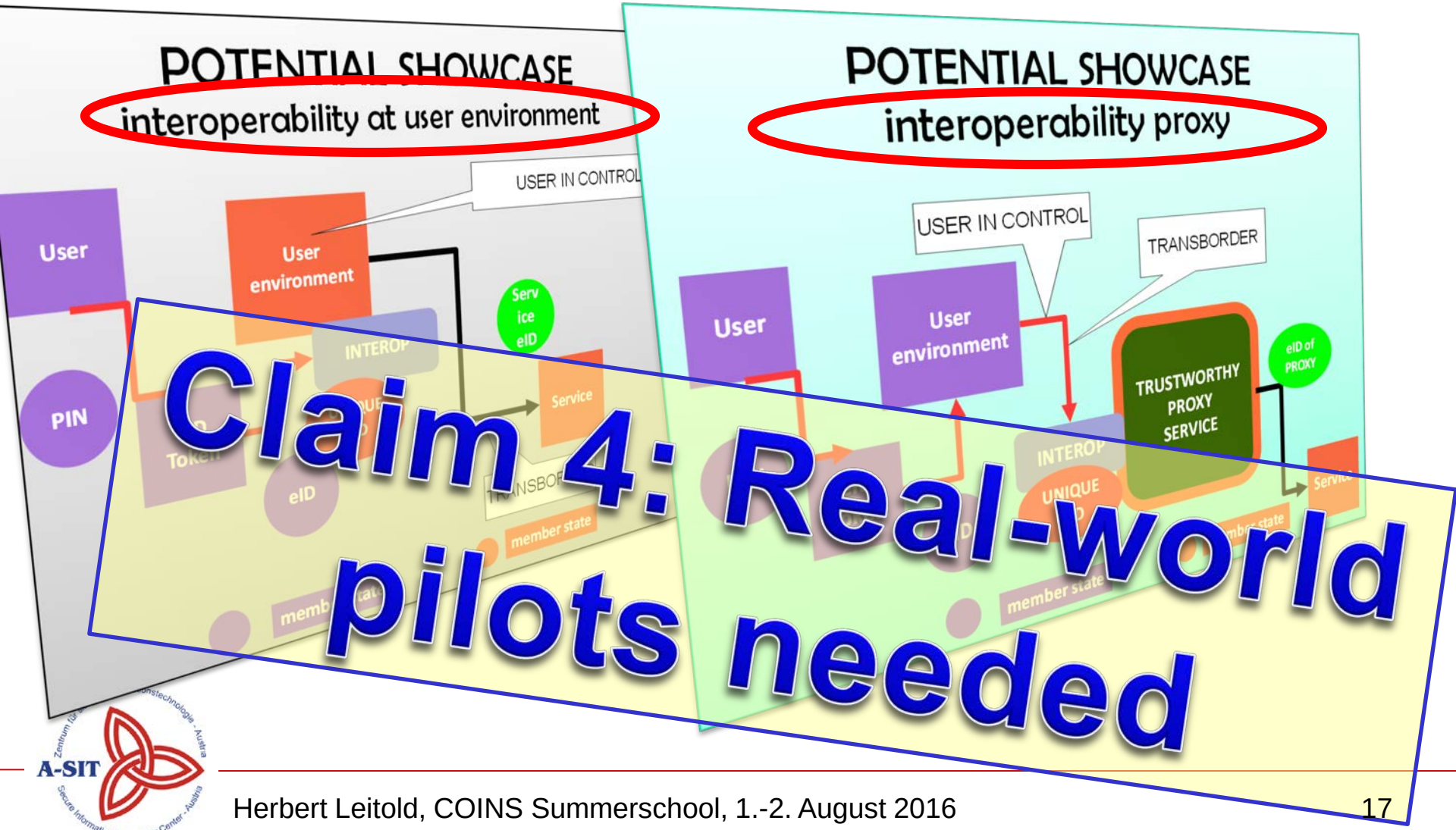
(2004-2005)

… developed signposts with a roadmap

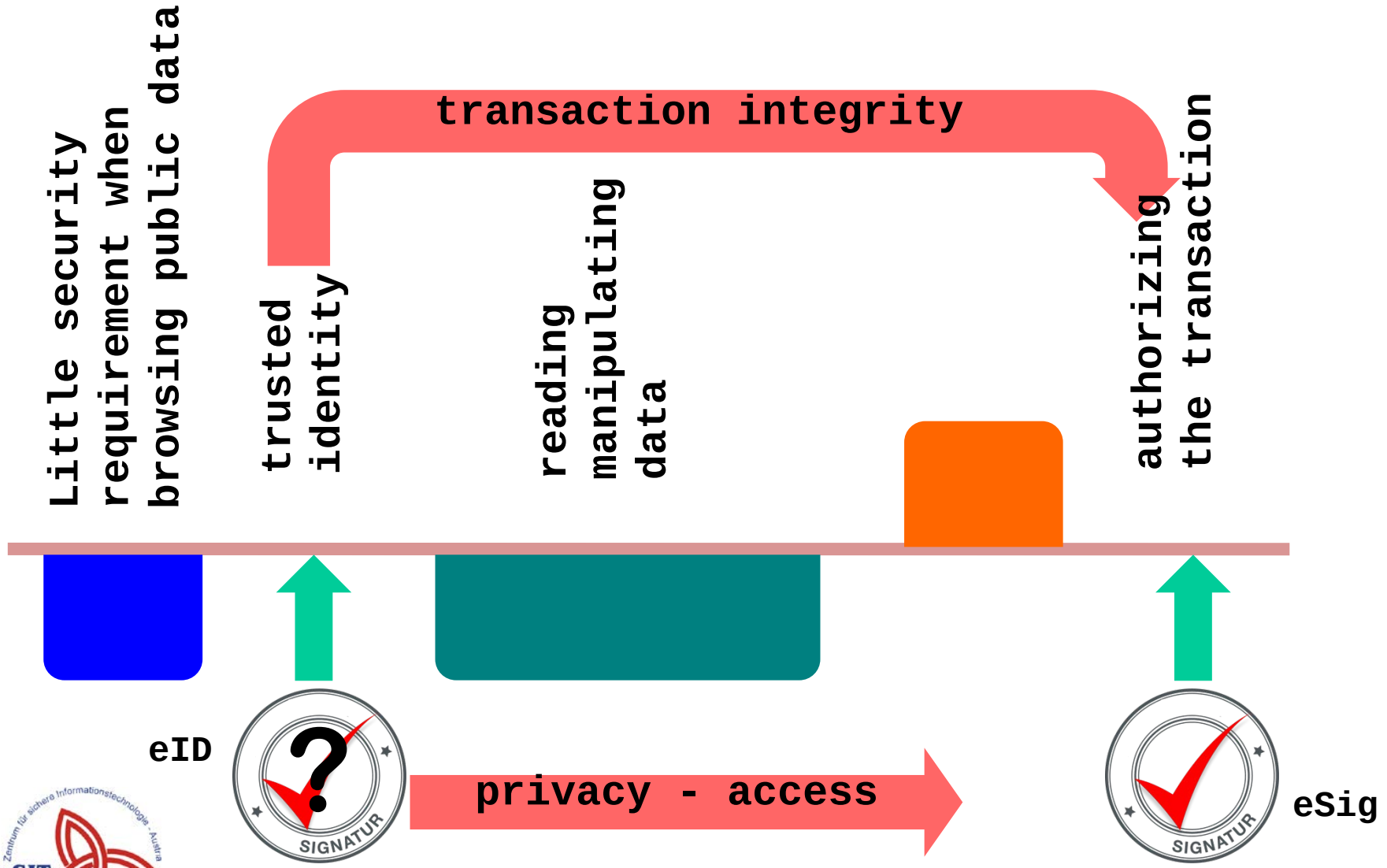


A little history: eID ad hoc-group

(2004-2005)

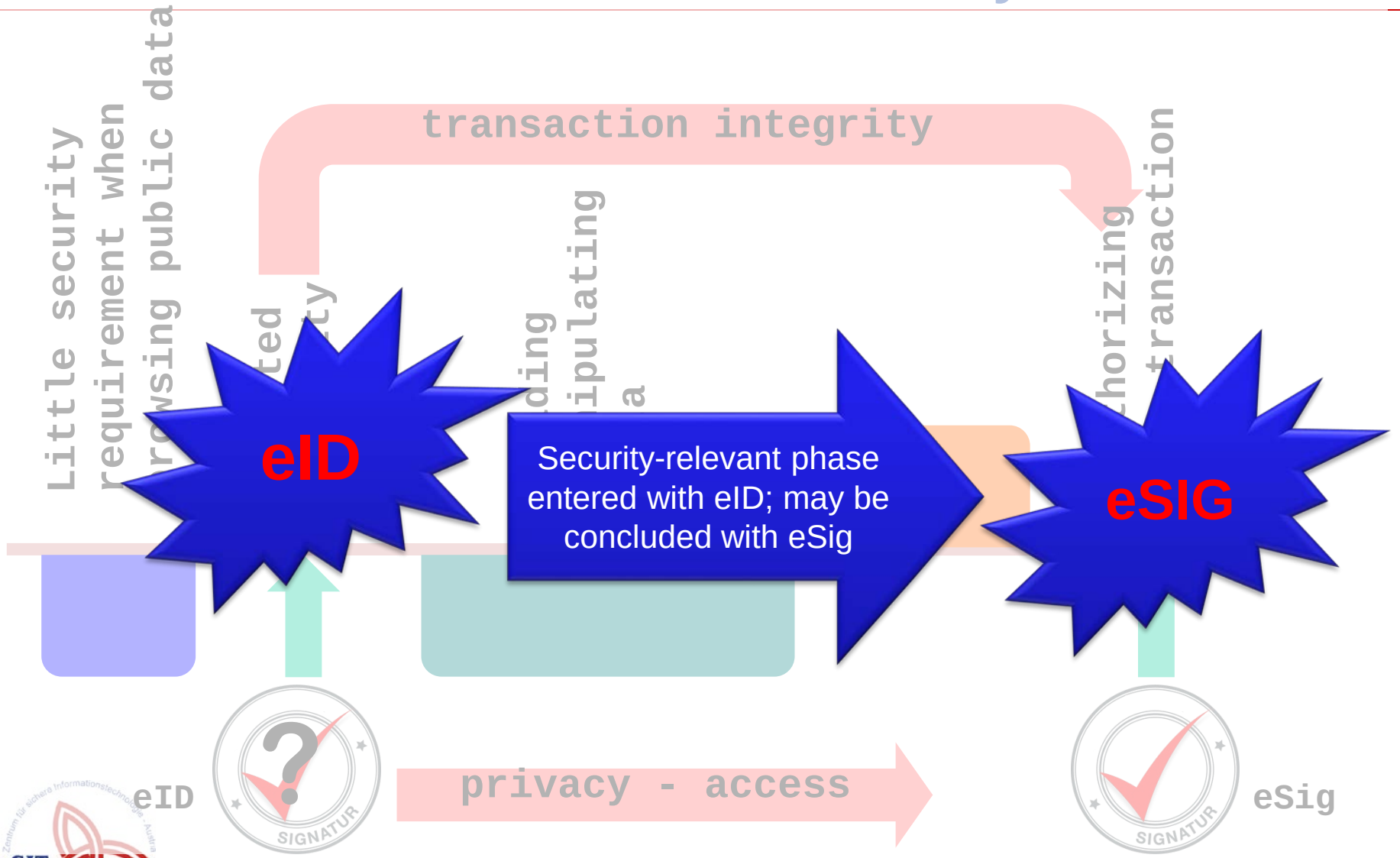


Citizen transaction and security



Source: Reinhard Posch, Major Cities, Wien 4.6.2012

Citizen transaction and security



SECTION 2: SOME NATIONAL CASE STUDIES

Overview

Country	ID card (physical)	eID means	National identifier
Austria	voluntary	Several *(voluntary)*	Yes – sector-specific
Estonia	obligatory	eID card (*obligatory*) mobiil ID (*voluntary*)	Yes – used “flat“
Germany	obligatory	nPA (*eID function voluntary*)	No – unconstitutional
Norway	?	ID-porten – federation	Fødselsnummer
United Kingdom	no	GOV.UK Verify – federation	No

Austria: Technologies

Smartcard

Bank cards
from 2005; ceased

Health insurance card
since 2005

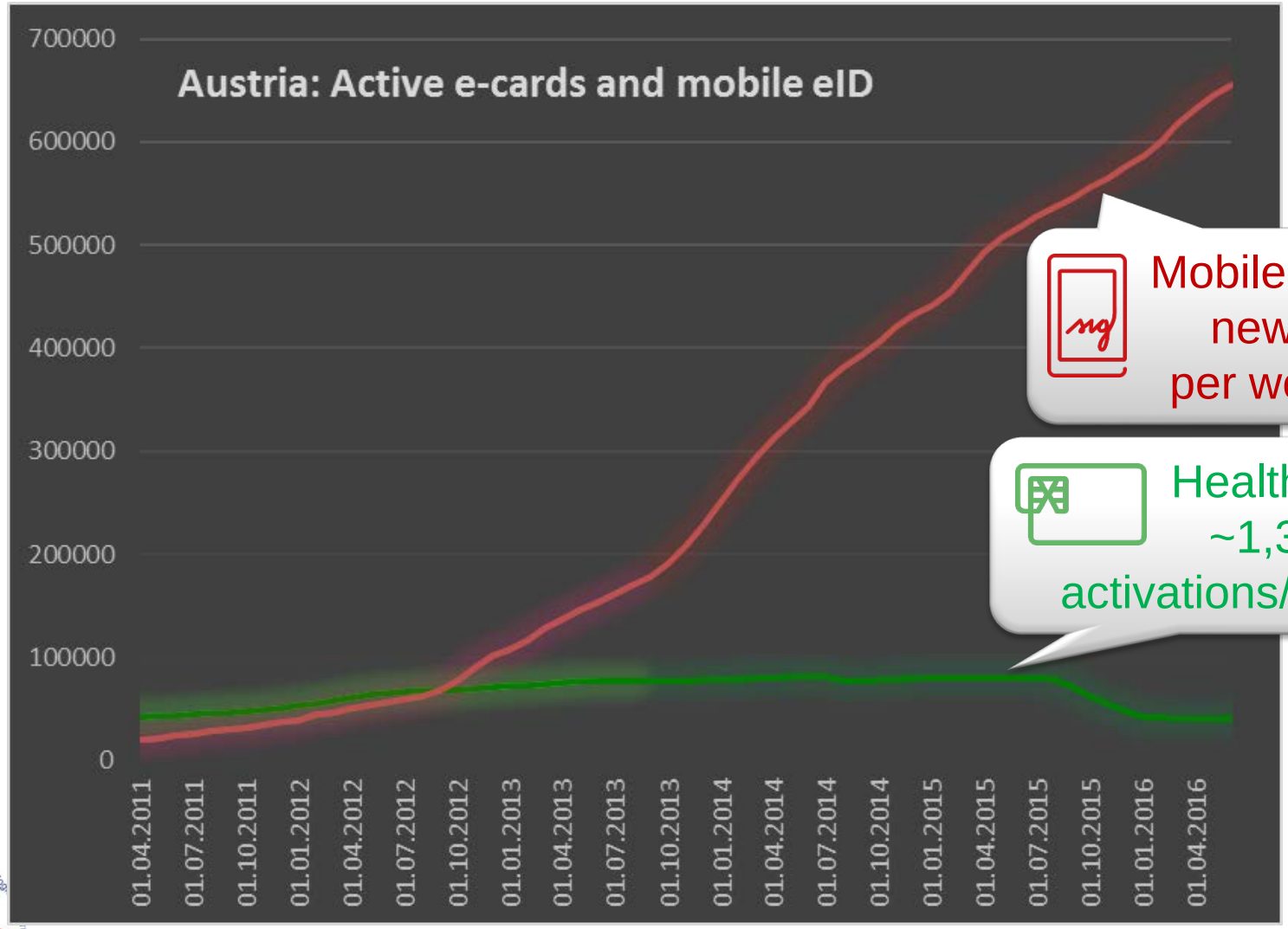
Profession cards, service cards, …
e.g. notaries, lawyers, ministries, …

Mobile

A1 signature
service by a MNO
from 2005; ceased in 2008
limited success

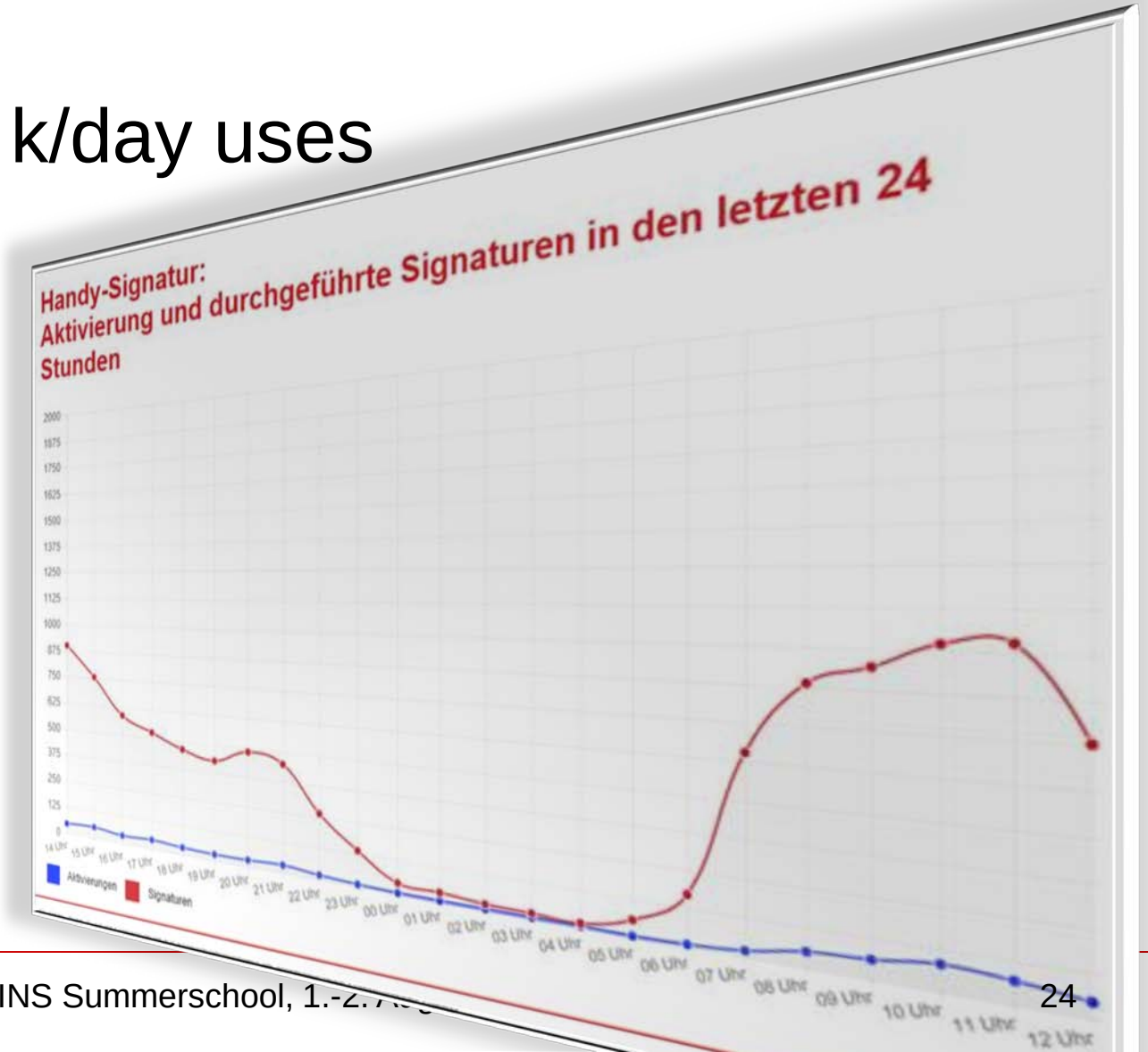
Mobile phone signature
Launched end 2009 through the LSP STORK
Contracted by gvmnt. to a private sector CSP
Success? Well, let's see ...

Austria: Card ID vs mobile ID



Austria: Actual usage … (mobile only)

- About 15-20 k/day uses on a typical working day
- ~4-6 k/day uses on weekends



Estonia

- Card eID introduced in 2002
  - 2015: ~100 mio. transactions

Statistics

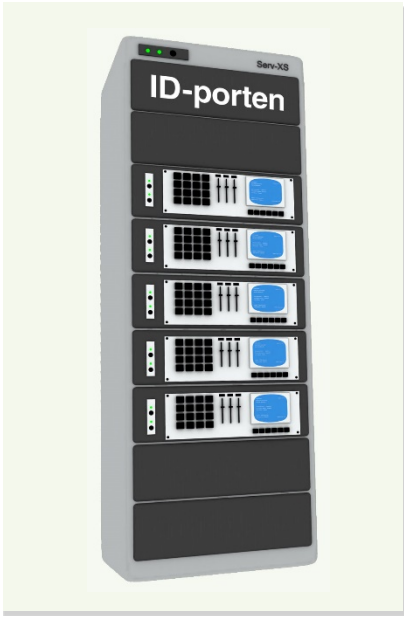
On 21.07.2016 08:18
Digital signatures **301 348 699**
Active cards: **1 272 213**
Electronic authentications: **457 826 295**

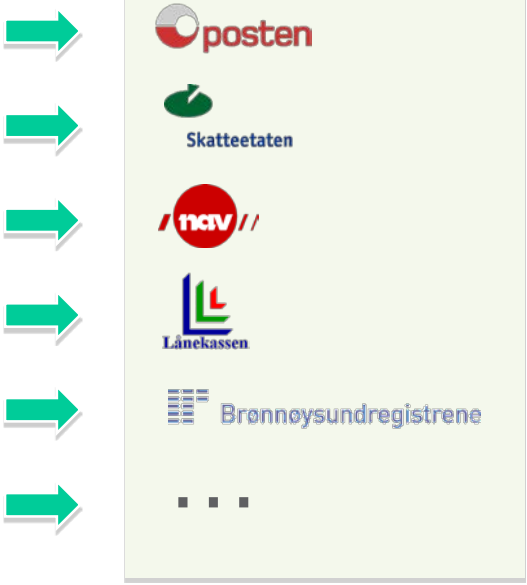
- Mobile ID since 2007 (crypto-processor on SIM)
  - Less than 10 % of ID card owners (growing fast)
  - 2015: ~25 mio. transactions

Germany

- nPA introduced in 2010
- All ID cards issued since can be enabled an "eID function" (voluntary)
  - About 1/3 of holders do so
- Some technical specifics
  - Contactless chip
  - Card-verified access certificate for relying parties
    - Minimum disclosure
    - Application specific identifiers; non-persistent (card-specific)

Norway





Nasjonalt ID-kort

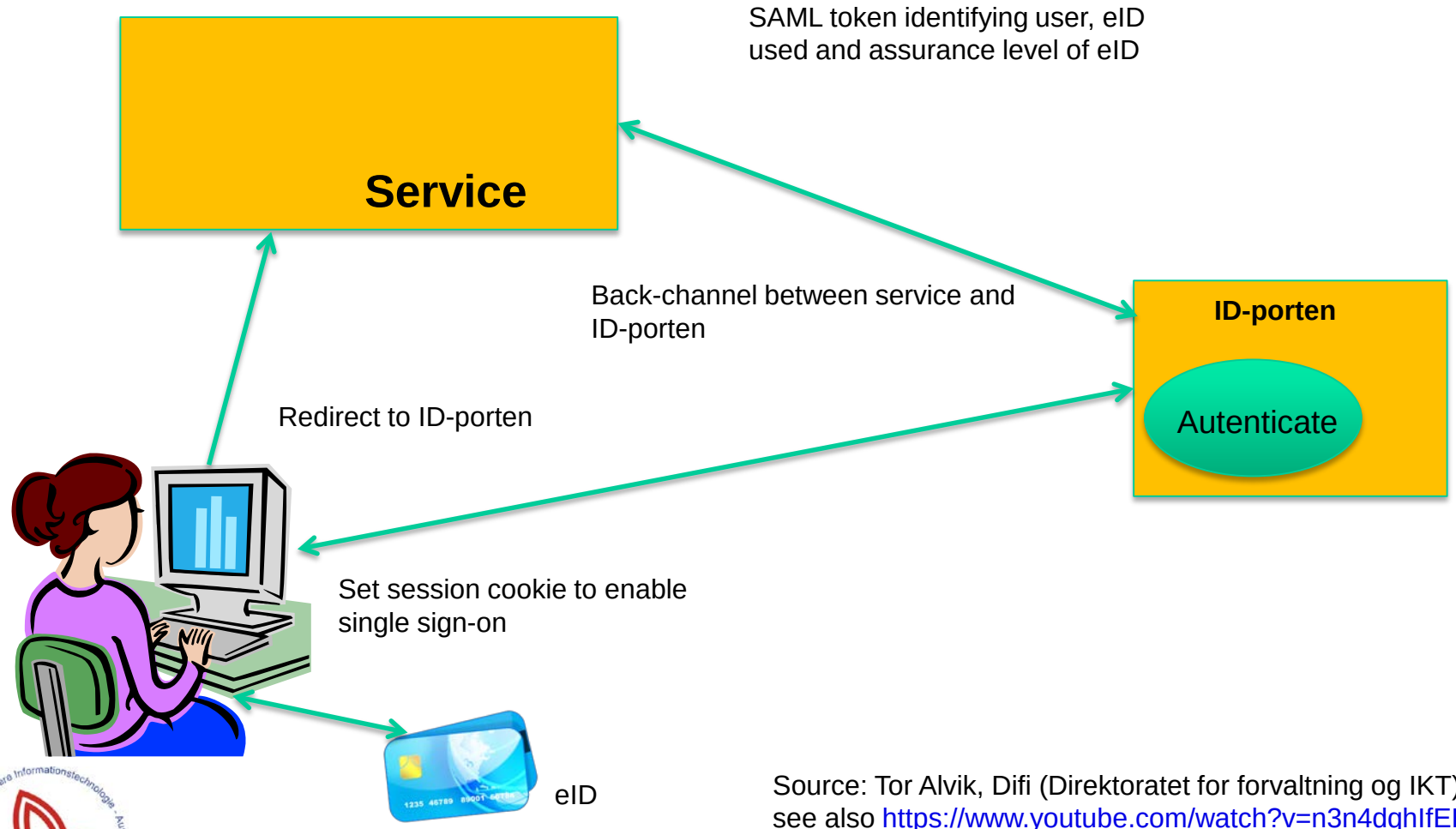
National ID-card with eID is planned for 2018

ID-porten authentication portal.
50 mill transactions in 2014

About 660 services from about 300 (?) public agencies

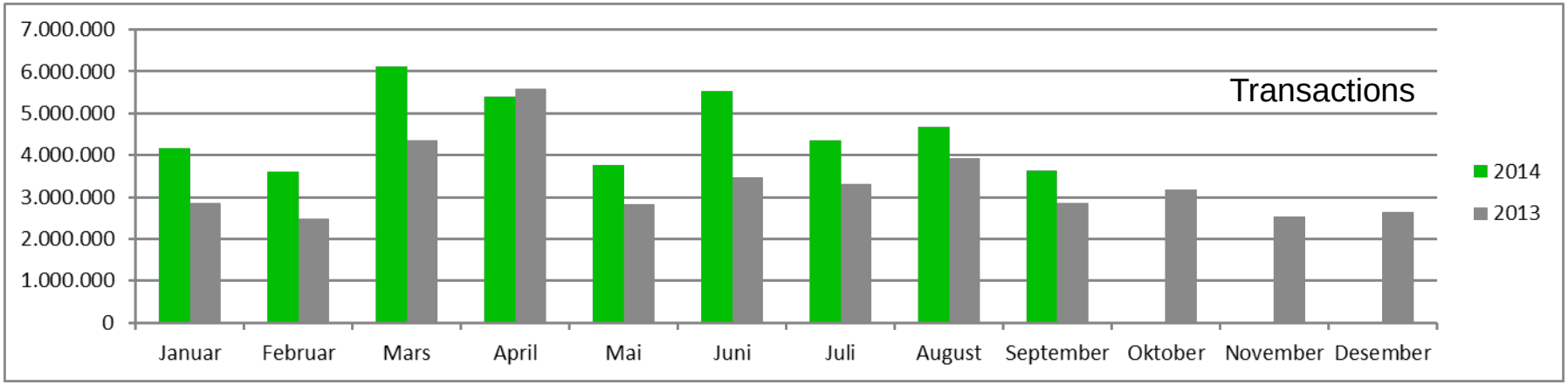
Source: Tor Alvik, Difi (Direktoratet for forvaltning og IKT)
see also https://www.youtube.com/watch?v=n3n4dqhIfEE

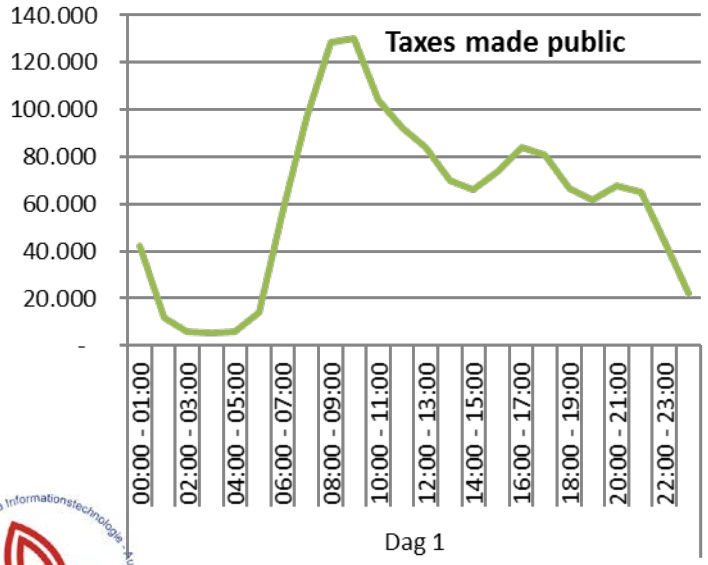
Norway: Authentication process



Source: Tor Alvik, Difi (Direktoratet for forvaltning og IKT)
see also https://www.youtube.com/watch?v=n3n4dqhIfEE

Norway: Facts and numbers





Source: Tor Alvik, Difi (Direktoratet for forvaltning og IKT)
see also https://www.youtube.com/watch?v=n3n4dqhIfEE

About the Nordics …

- For a good overview of DK, FI, IS, NO, and SE see the study:

  Kjell Hansteen, Jon Ølnes, Tor Alvik
  „Nordic digital identification (eID)“

Available at
http://norden.diva-portal.org/smash/record.jsf?pid=diva2%3A902133&dswid=8002

Remember …

Country	ID card (physical)	eID means	National identifier
Austria	voluntary	Several (*voluntary*)	Yes – sector-specific
Estonia	obligatory	eID card (*obligatory*) mobiil ID (*voluntary*)	Yes – used "flat"
Germany	obligatory	nPA (*eID function voluntary*)	No – unconstitutional
Norway	?	ID-porten – federation	Yes (Fødselsnummer)
United Kingdom	no	GOV.UK Verify – federation	No

There are differences. In a cross-border context, one either could

- **harmonise, or**
- **cope with these differences**

The lecture will deal with the latter

SECTION 3: TERMINOLOGY

Gratitude to my colleague Bernd Zwattendorfer, who provided his lecture slides "*Selected Topics IT-Security 1*"

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]

- Appears where the proof of being a particular person or having specific attributes or properties are required
- Identity describes a person's unique and distinctive characteristics, distinguishing them from one another
  - Name, gender, color of hair and eyes, …
- Identity is often also referred to as *principal*, within a digital context as *subject*

Digital Identity

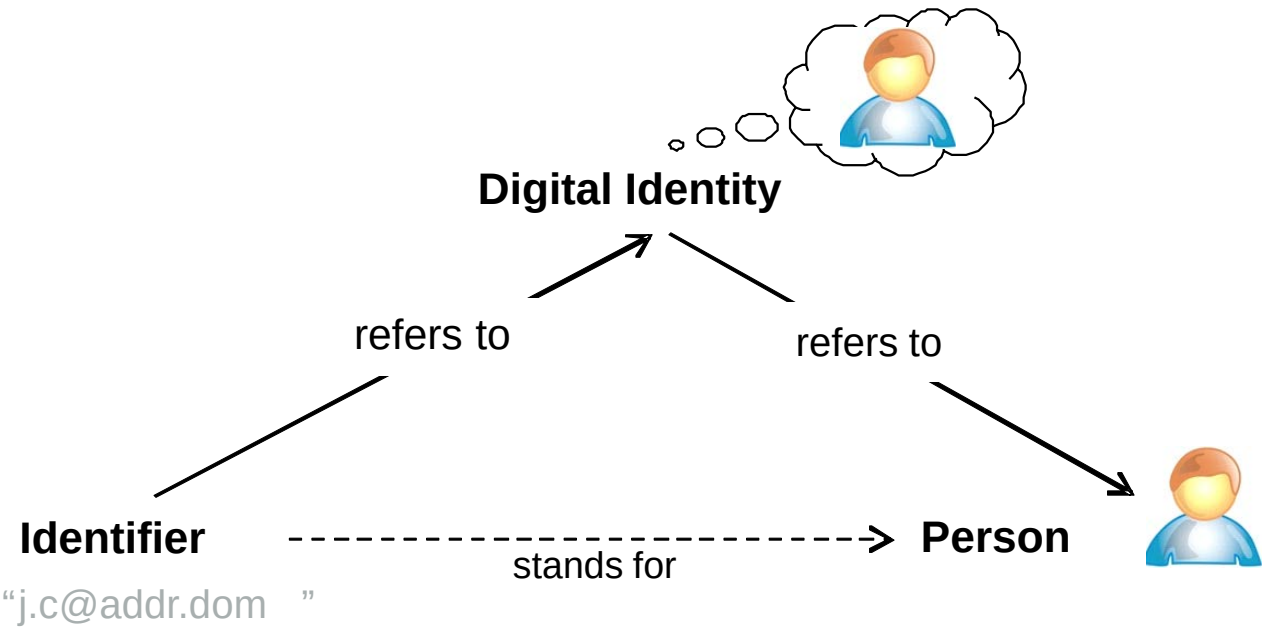
"Digital identity can be defined as the digital representation of the information known about a specific individual or organization. [Bertino and Takahashi]

„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]

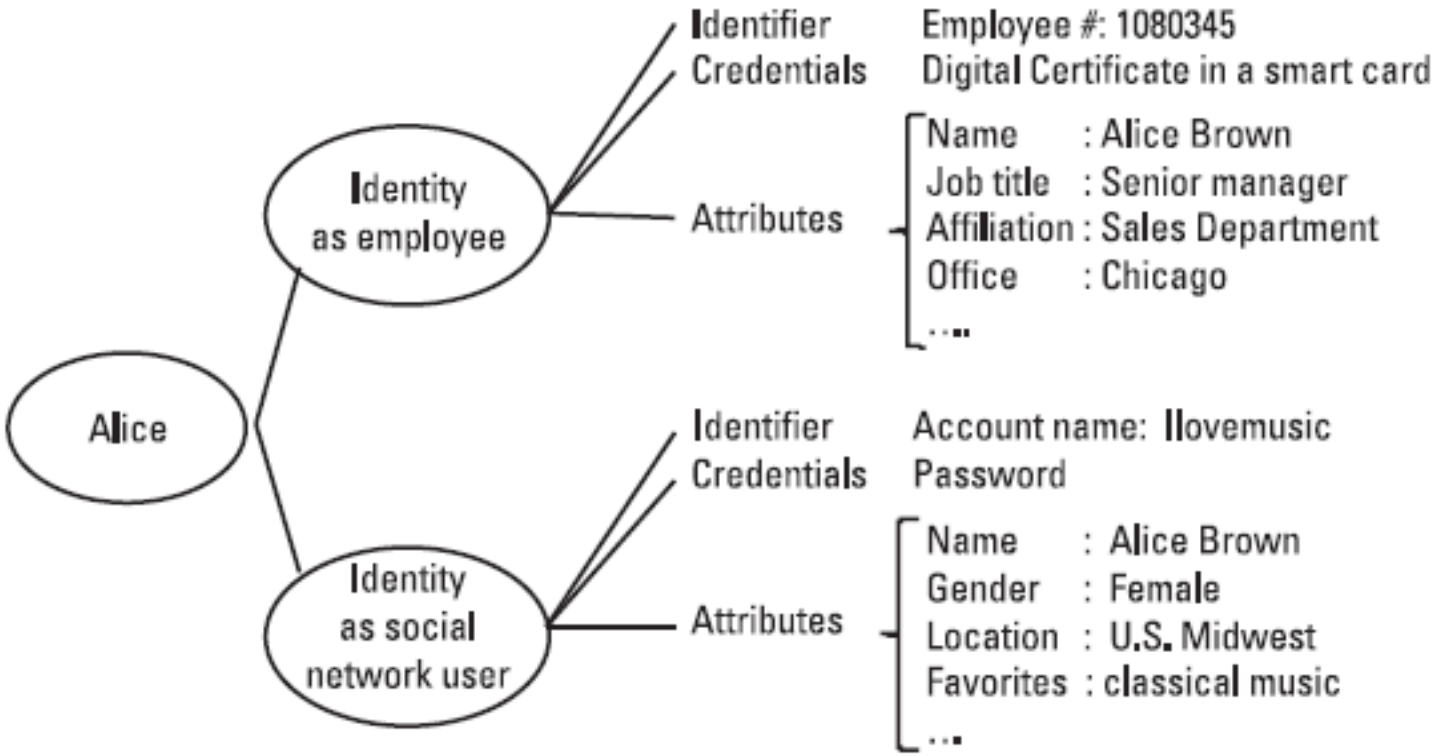
- Same identity properties and attributes, but digitally available
  - E.g.: name, date of birth, …
  - Also: username, e-mail, …
- Applicable also to non-natural persons
  - E.g. a company, …

Digital Identity | Triangle



Ref: GINI-SA

Several Digital Identities



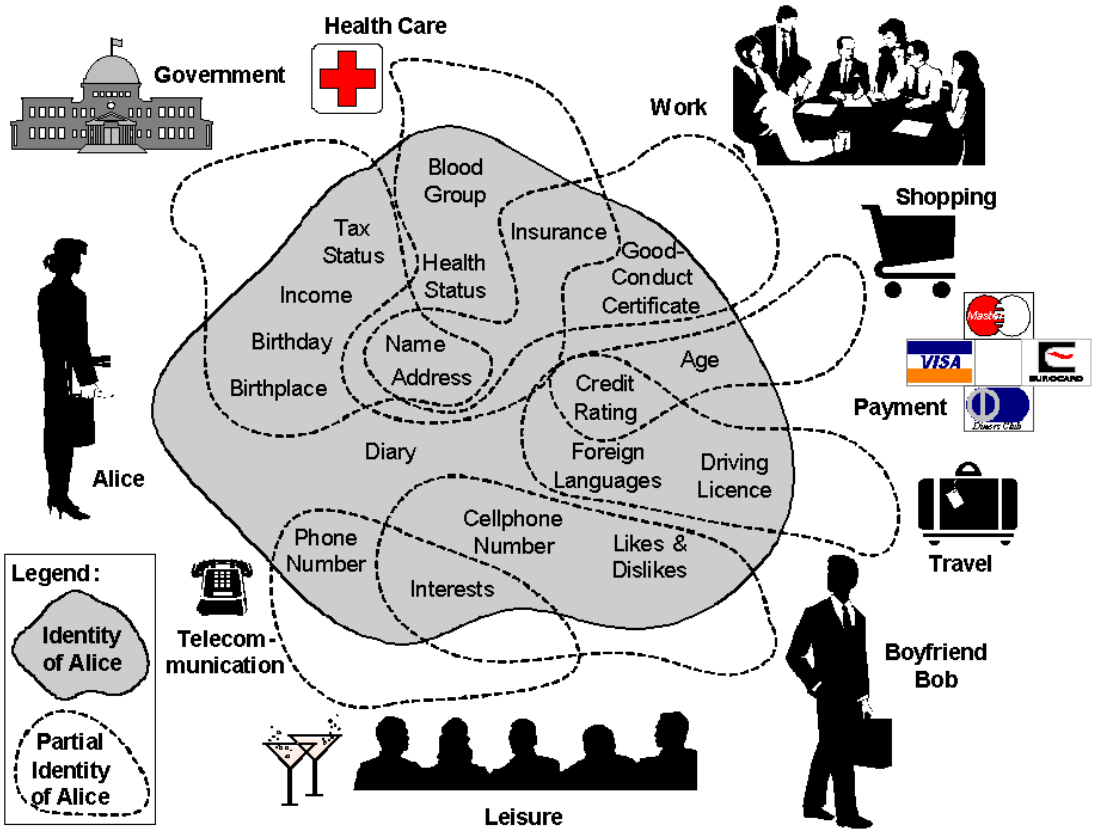
Ref:
Bertino/Takahashi

Digital Identity

- Identifier
  - Character string identifying a person
  - May be restricted in time or in the application sector
  - E.g.: username, e-mail, URI, tax number, social security number, ..
- Credentials
  - Credentials for parts or complete identity
  - Used for proving identifier and/or attributes
  - E.g.: password, certificate, …
- Attributes
  - Describing a person's properties
  - E.g.: name, date of birth, gender, …

Identity Types

- Complete identity
  - Union of all attribute values of all identities of this person
- Partial identities
  - Different set of attributes forming identities (e.g. at work, social media, …)



Ref: FIDIS

Identity Types

- Pseudonymous identities
  - Decoupling of the digital identity from the real person (by a trustworthy entity)
  - Only the trustworthy entity is able to link back to the real person
  - E.g. name changed by editorial office
  - E.g. Used for analysis of health data
- Anonymous identities
  - Decouple the digital identity from the real person
  - Unlinkability to real person
  - Normally temporary and for single transactions
  - E.g. completing a questionnaire

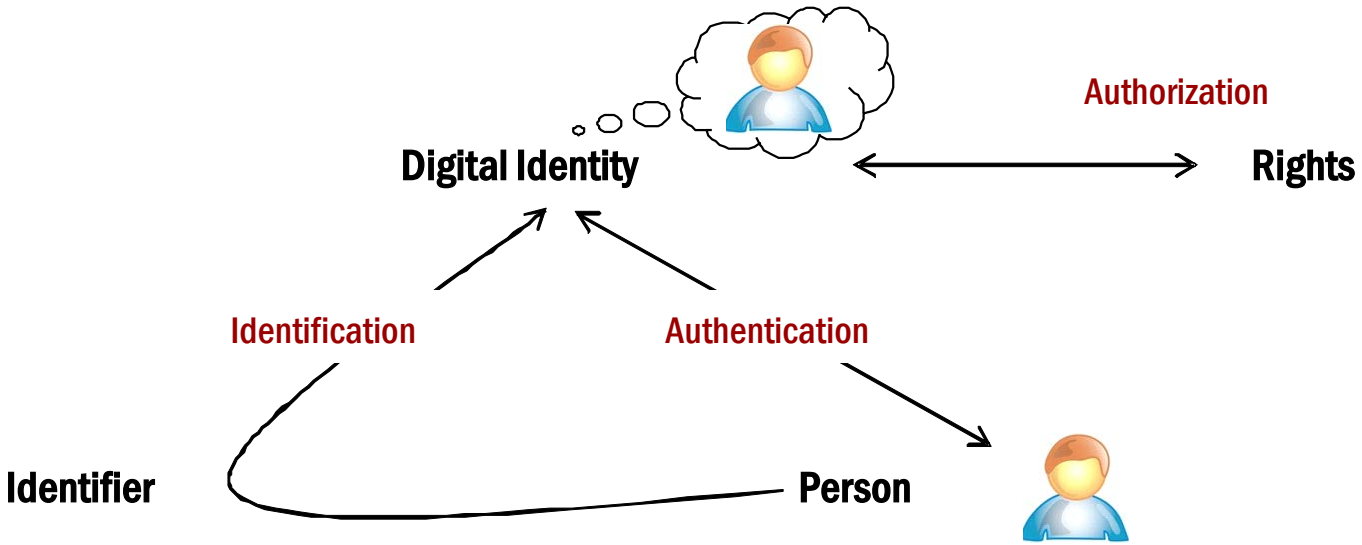
Identity Types

- 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
  - Allows systems the shared usage of identity data
  - Single sign-on (SSO)
- Brokered identity
  - Identity translation
  - E.g. from partial identity to pseudonymous identity because of privacy reasons

Electronic Identity (eID)

- Aims to guarantee the unique identity of a person (natural or legal person) ensuring trust between parties involved in electronic transactions
- Particularly required in sensitive areas of applications
  - e.g., e-Health
  - e.g., e-Government
- I-S-A functions
  - **I**dentification, **S**ignature, **A**uthentication
- Features that need to be supported by an eID
  - universal coverage, uniqueness, persistence, exclusivity, precision

Identification | Authentication | Authorization

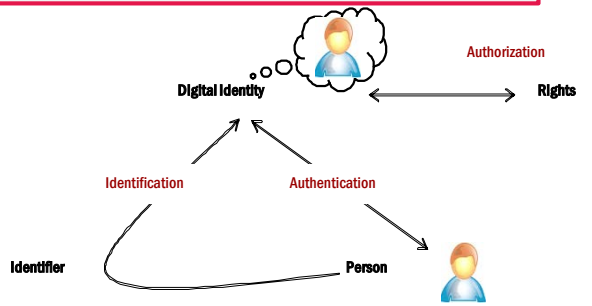


Ref: GINI-SA

Identification, electronic identification

"Identification": Identification is the association of a personal identifier with an individual presenting attributes. [Clarke]

"Electronic Identification": means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person; [eIDAS]



- Formerly: People knew each other
- Traditional: ID card
  - Passport, identification card, driving license, …
- Online: Electronic ID (eID), e.g. Austrian Citizen Card, Estonian eID, Norwegian ID-porten, …

Identification

- An association between a personal attribute and an individual, that represents different properties
- E.g.: The name “John Doe” identifies the person “John Doe”.
- Unique identification is only possible if no other person’s name is “John Doe” (within a defined context)
  - Else additional attributes are required for unique identification (e.g. date of birth, address, …)

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

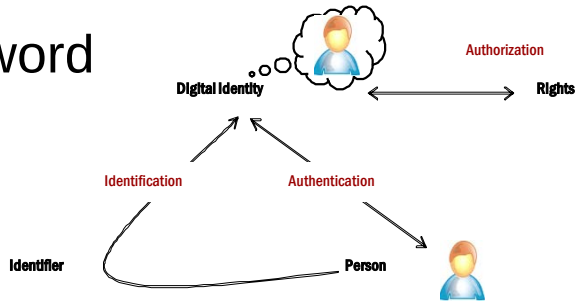
Authentication is proof of an attribute. [Clarke]

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]

An electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;. [eIDAS]

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



Authentication mechanisms

- "Having something" approach (ownership)
  - Authentication based on "something" an entity owns or has for proving her identity.
  - E.g., passport, smart card, private key
- "Knowing something" approach (knowledge)
  - Authentication based on presented knowledge
  - E.g., password, PIN
- "Being something" approach (physical property)
  - Authentication based on physical property
  - E.g., fingerprint
- "Doing something" approach (behavior pattern)
  - Authentication based on something an entity does
  - E.g., voice recognition

Multi-Factor-Authentication

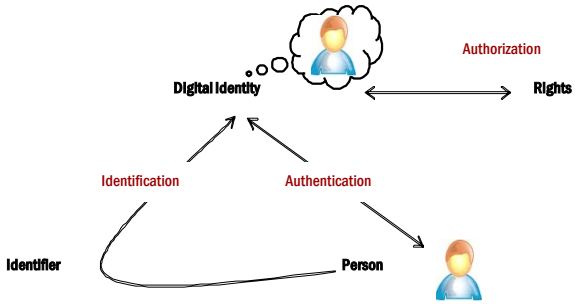
- Combining different authentication mechanisms to increase security
- E.g. Ownership and Knowledge (2-factor)
  - Citizen card (smart card and PIN)
  - Mobile phone signature (mobile phone and password)
- Increased security by increasing the number of mechanisms

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 access rights to particular resources or entities
  - E.g. Read-/write rights on file system
- Often based on roles or groups
  - E.g., doctor, student, etc.



Exceptions

- Identification without authentication
  - Doctor wants to access patient's data
  - Doctor identifies herself, authenticates herself and gets adequate access rights
  - Patient is only identified
- Authentication without identification
  - Anonymous credentials (AC)
  - Prove that someone is older than 18 without revealing other identifying attributes

Identification, Authentication, Authorization

Summary

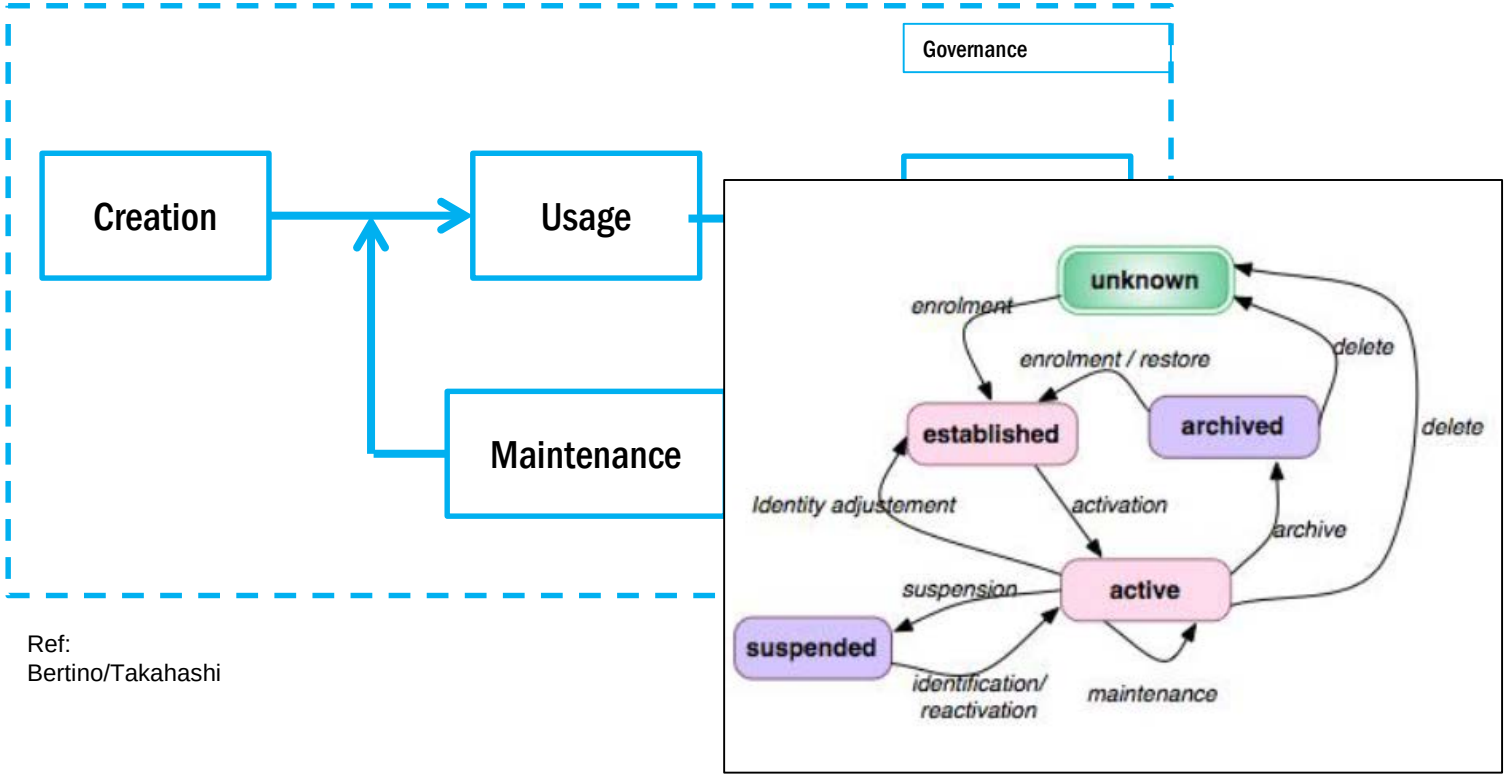
- Identity
  - “Jane Doe“
- Identification
  - “I am Jane Doe“
- Authentication
  - “My passport proves that I am Jane Doe”
- Authorization
  - “Jane Doe is employed at company A and is allowed to access service B”

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 Lifecycle



Ref:
Bertino/Takahashi

Ref: ISO/IEC 24760-1

Identity Lifecycle

- Creation
  - Create data record of the digital identity
    - Contains different attributes
    - Attributes may be
      - self-created, self-declared
      - proved and verified
  - Credential is issued

Identity Lifecycle

- Usage
  - Used in different (personalized) services
  - Authentication and authorization
  - Transfer/Distribution to other systems (e.g. other companies) respectively system parts (e.g. internal registers/databases)
  - Single sign-on (SSO)

Identity Lifecycle

- Maintenance
  - Attributes and their values may change
    - e.g. address
  - Attributes may be added or deleted
  - Attributes may have limited validity
    - e.g. certificate valid for 1 year
  - Identifiers should not be changed
    - But happens in real life (also national eID schemes)

Identity Lifecycle

- Deletion
  - Validity period may expire (e.g. certificates)
  - Validity may be revoked (e.g. certificates)
  - Simple deletion
  - Revocation should be documented and other systems should be informed

Identity Lifecycle

- Governance
  - Policies/guidelines for creation, usage, maintenance and deletion of identities
  - Policies/guidelines for authentication (e.g. LoA)
  - Policies/guidelines for authorization (e.g. conditions for data access)
  - Legal framework
  - Audit – traceability of single activities

Levels of Assurance

- Assurance level of the transmitted identity data
- Quantitative representation of identity enrolment, credential, authentication process, etc.
- Grounded by risk assessment of applications
- Different, but related approaches
  - NIST SP 800-63: Levels of Assurance (4 levels)
  - ISO/IEC 29115: Levels of Assurance (4 levels)
  - STORK: Quality Authentication Assurance Level (4 levels)
  - eIDAS: Levels of Assurance (3 levels)
  - For natural persons, legal persons, machines, …

ISO/IEC 29115

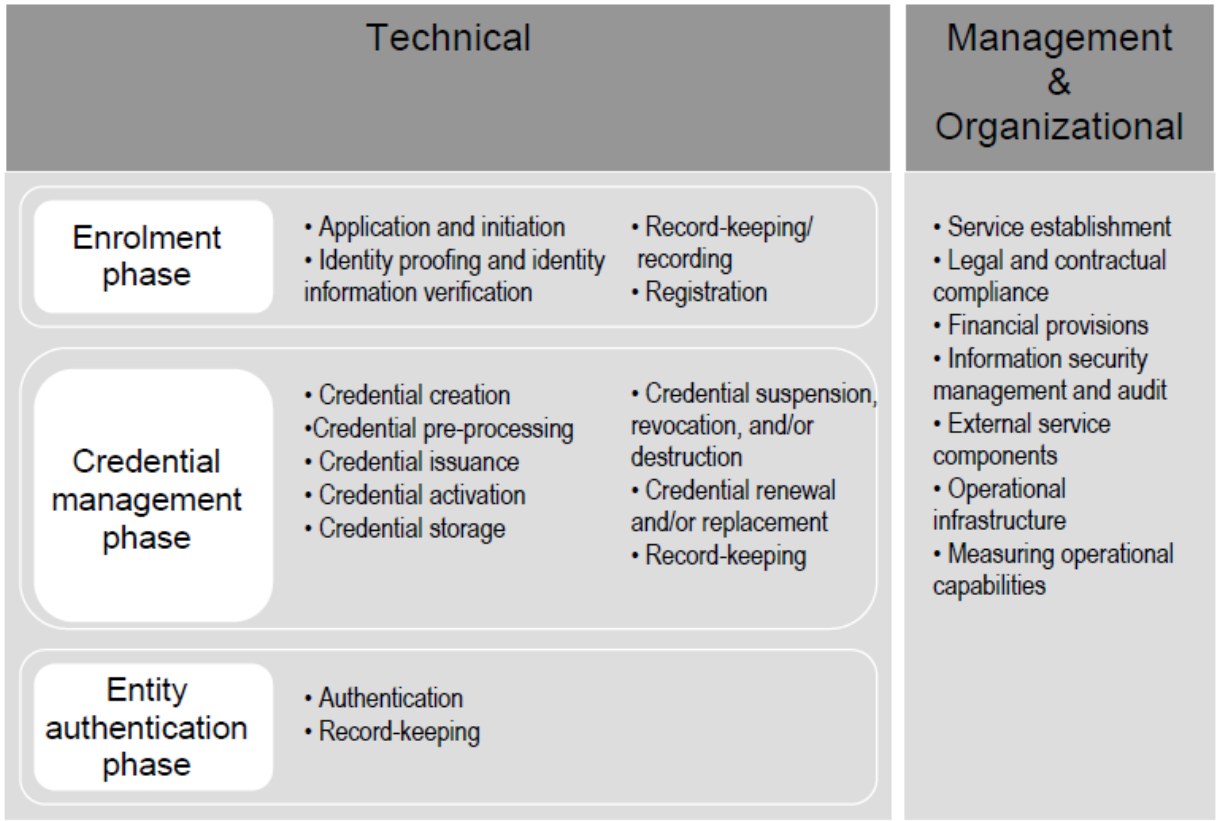
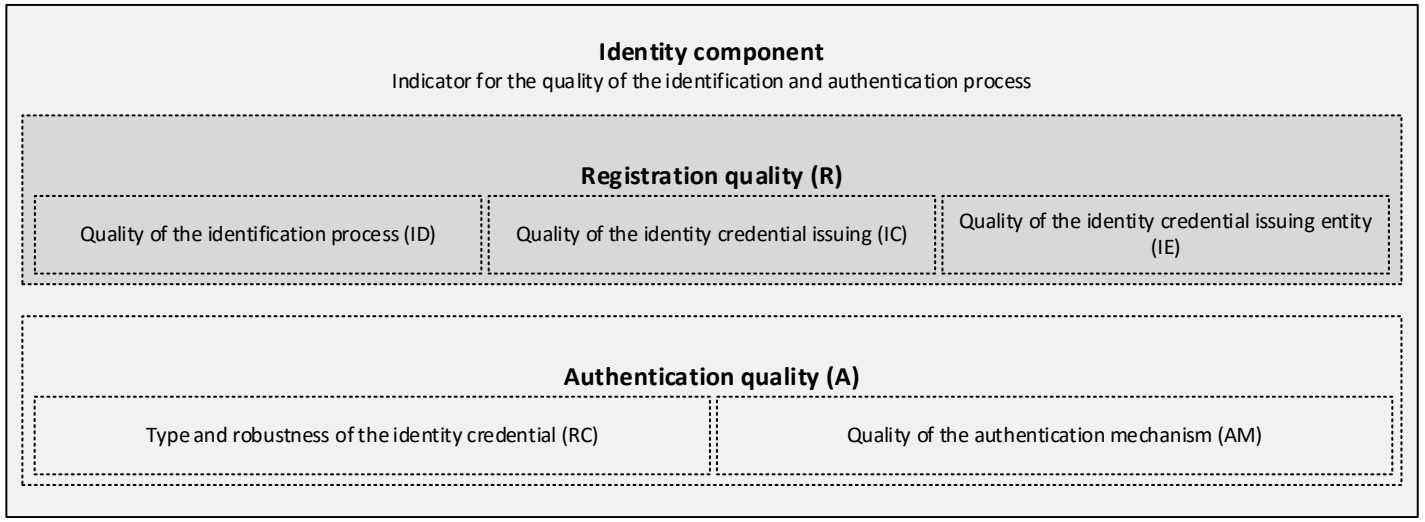


Figure 1 — Overview of the Entity Authentication Assurance Framework

Austrian SecClass

- An example of a national scheme



Austrian SecClass (2/3)

Component	Minimal requirements to the components
Quality of the identification process (ID)	The person has to be physically present in the registration process at least once. AND Stating multiple attributes (e.g. name and date of birth) that allow unique identification. AND The identity is validated using a legal identity document including at least a photograph or a signature (passport, driving licence, …). The data may be validated using trustworthy instruments.
Quality of the identity credential issuing (IC)	The person receives the identity credential after the identification process personally from the identifying instance. OR The identity credentials are forwarded by mail and are activated after the identification process.
Quality of the identity credential issuing entity (IE)	The CSP is a public entity (public authority or agency). OR The CSP has qualifications according to Annex II of the EU-Directive 1999/93/EC respectively § 7 SigG.
Type and robustness of the identity credentials (RC)	Identity credentials based on a qualified hardware-certificate according to Annex I of the EU-Directive 1999/93/EC. (Citizen Card)
Quality of the authentication mechanism (AM)	Secure authentication mechanisms, based on state-of-the-art technology, providing protection against most common threats.

Austrian SecClass (3/3)

Quality of the identification process (ID)……	4
Quality of the identity credential issuing (IC)……	3
Quality of the identity credential issuing entity (IE)……..	4
Registration Quality (R)……	3
Lowest quality level out of ID, IC and IE	
Type and robustness of the identity credential (RC) ……..…	4
Quality of the authentication mechanism (AM)……..	2
Authentication quality (A)……..	2
Lowest quality level out of RC and AM	
Overall quality identity component ……	2
Lowest quality level out of R and A	

eIDAS - LoA

- Further discussed in the final session

- 3 levels *low*, *substantial*, and *high*
- Distinguished through quality of:
  - Enrolment
  - eID Means management
  - Authentication
  - Management and Organisation

Identity Threats

- Identity linking
  - Information regarding an identity is collected and a profile is derived
  - 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. Intentional or unintentional disclosure of health data

Ref:
Tsolkas/Schmidt

Challenges for Digital Identity

- Security
  - To counter 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

SECTION 4: LAWS OF IDENTITY

… by Kim Cameron (2005); see also http://www.identityblog.com/

The Laws of Identity

- Seven elements est. through blog discussions
  1. User Control and Consent
  2. Minimal Disclosure for a Constrained Use
  3. Justifiable Parties
  4. Directed Identity
  5. Pluralism of Operators and Technologies
  6. Human Integration
  7. Consistent Experience Across Contexts

The Laws of Identity: #1 - #2

1. **User Control and Consent**
   "*Technical identity systems must only reveal information identifying a user with the user's consent.*"

2. **Minimal Disclosure for a Constrained Use**
   "*The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.*"

The Laws of Identity: #3 - #4

3. Justifiable Parties

"*Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.*"

4. Directed Identity

"*A universal identity system must support both 'omni-directional' identifiers for use by public entities and 'unidirectional' identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.*"

The Laws of Identity: #5 - #6

5. **Pluralism of Operators and Technologies**
   "A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers."
6. **Human Integration**
   "The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks."

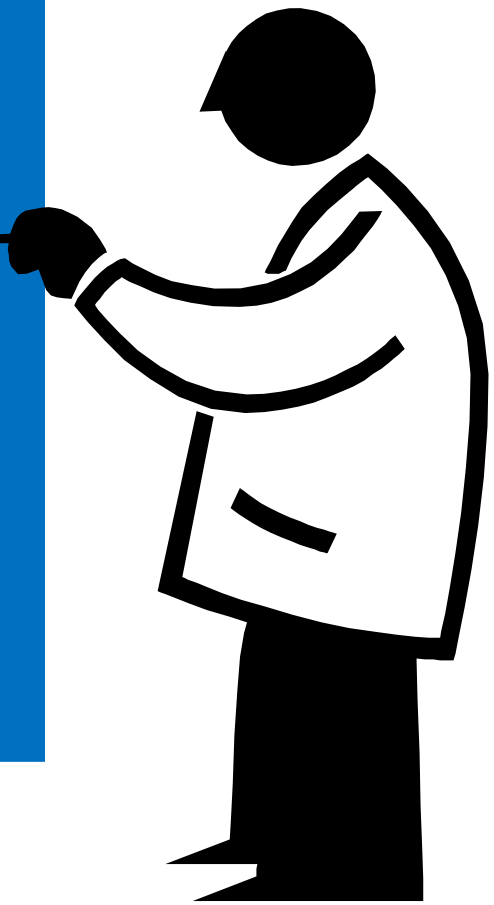
The Laws of Identity: #7

7. Consistent Experience Across Contexts

"The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies."

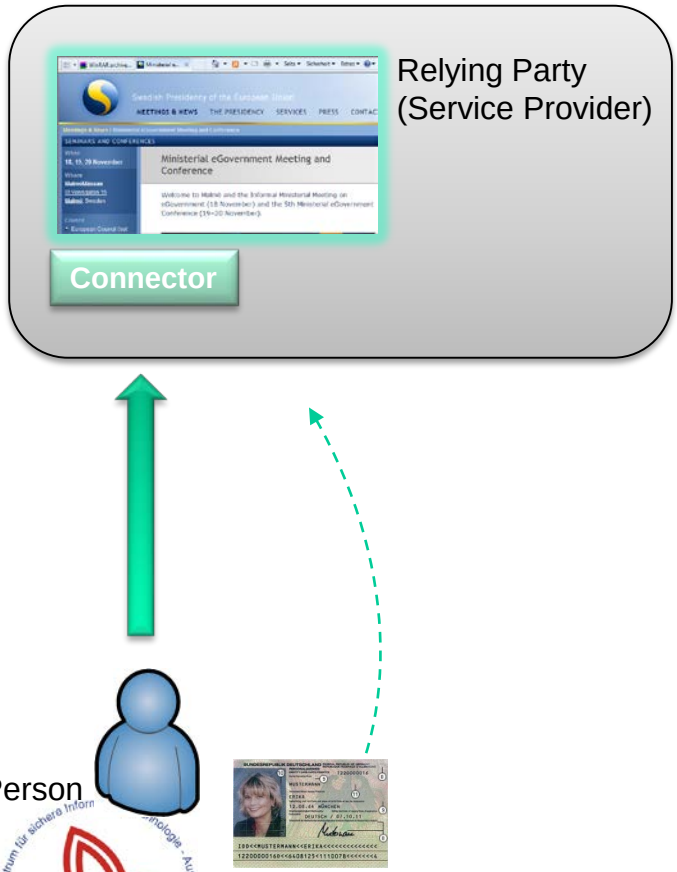
Contents

- Motivation, Terminology
- **Federation Protocols**
  - *Architectures*
  - *SAML, OAuth, CAS*
- STORK and STORK 2.0
- eIDAS



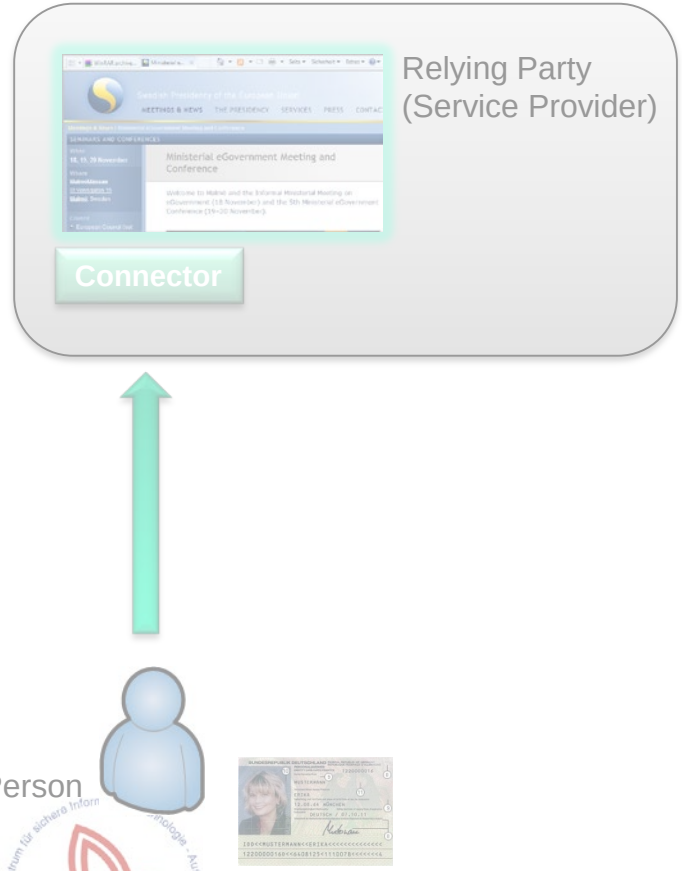
Direct vs. Indirect authentication

Direct Authentication

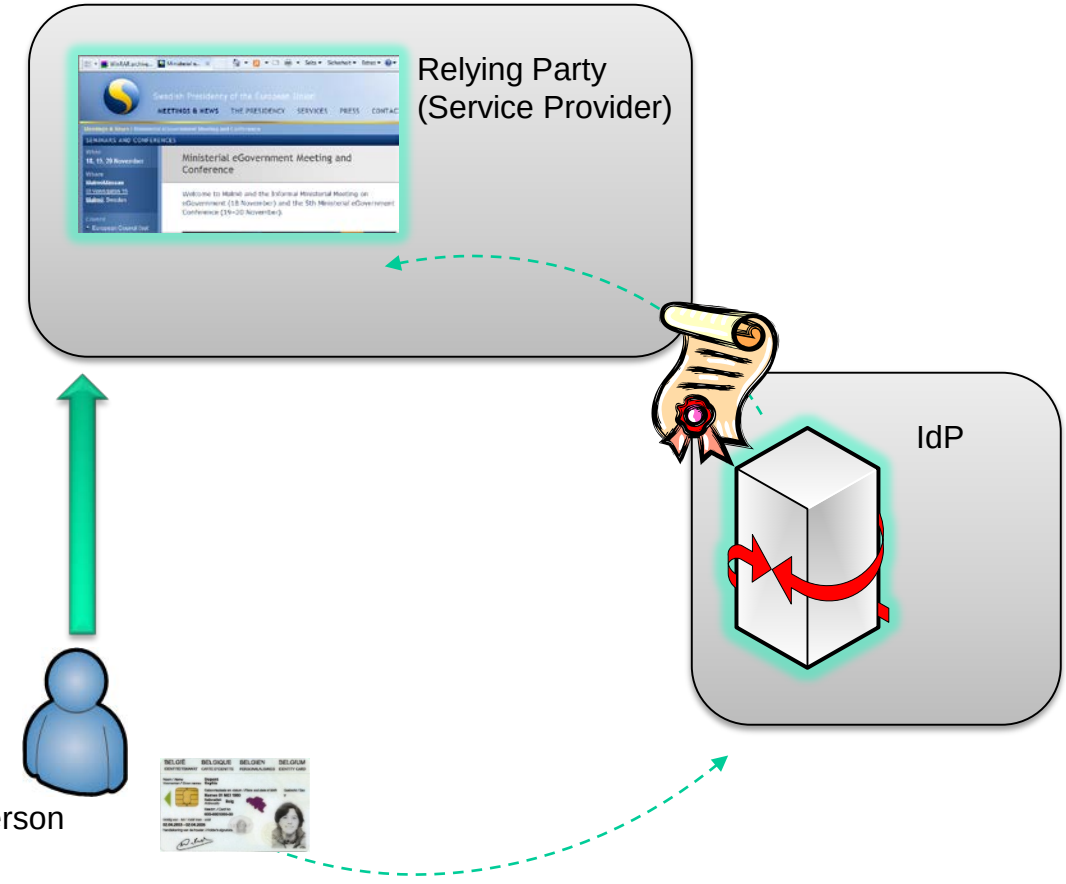


Direct vs. Indirect authentication

Direct Authentication

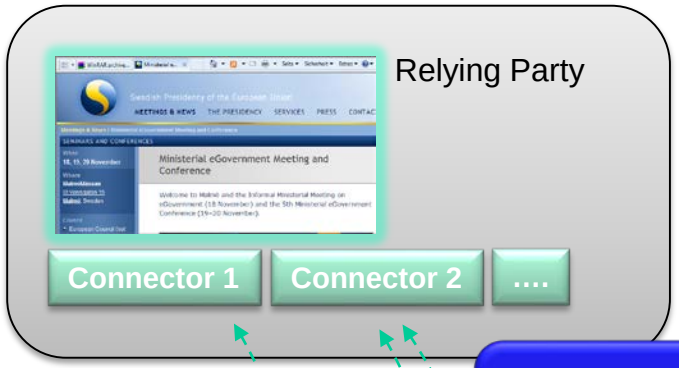


Indirect (IdP-based) Authentication

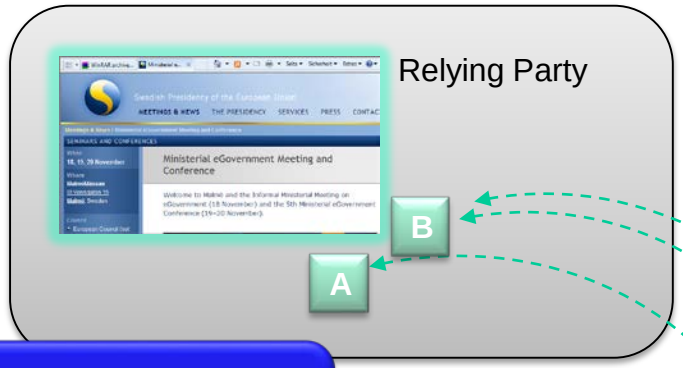


What if there are several eID schemes?

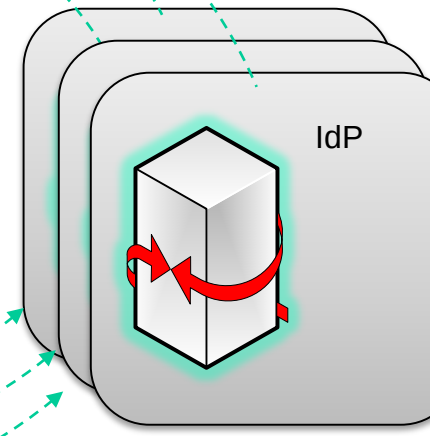
Direct Authentication

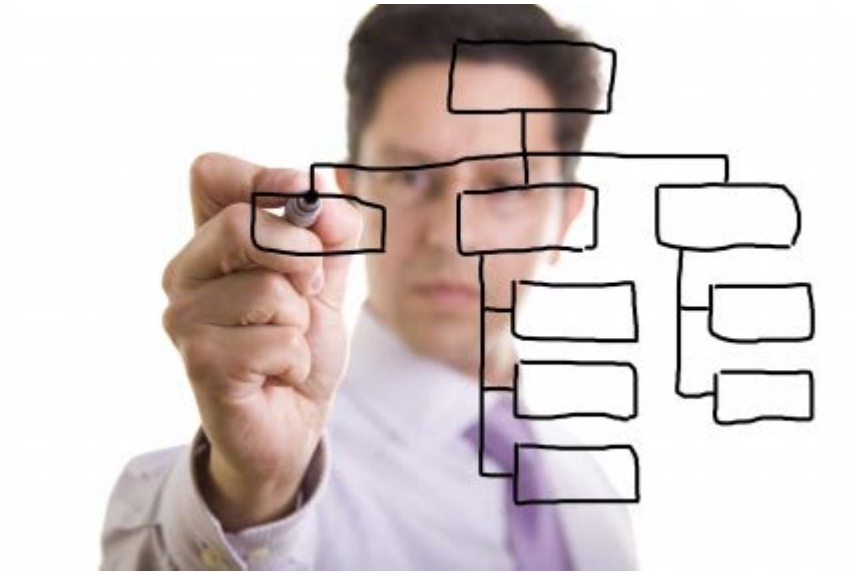


Indirect (IdP-based) Authentication



Scalability in both cases depends on variety and/or use of standards

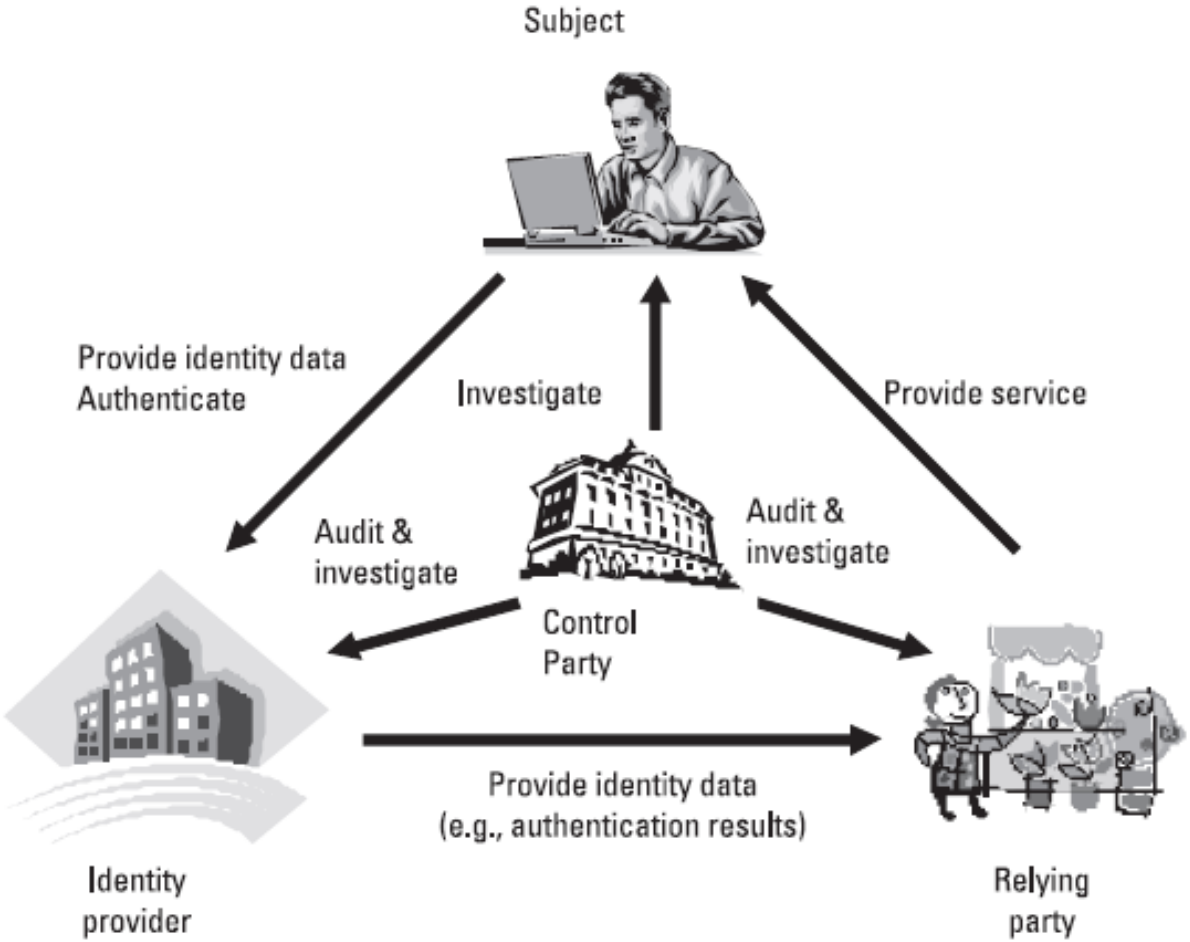




SECTION 5: ARCHITECTURES

Gratitude to my colleague Bernd Zwattendorfer, who provided his lecture slides "*Selected Topics IT-Security 1*"

Stakeholders

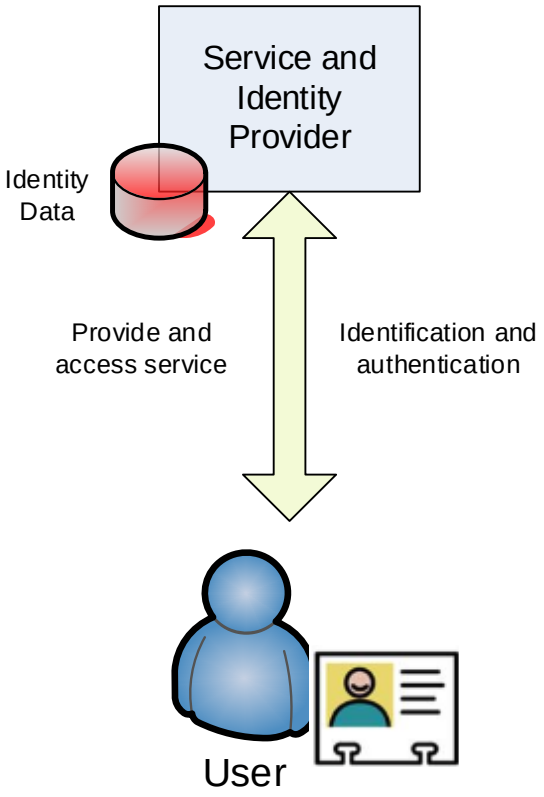


Ref:
Bertino/Takahashi

Stakeholders

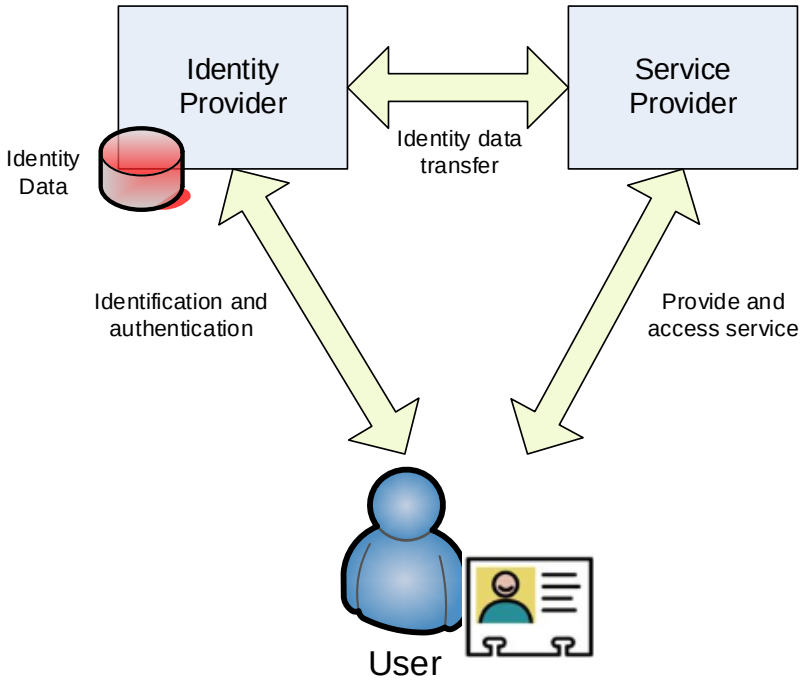
- Subject
  - Digital identity of a person
  - Provides identity data (attributes) to the identity provider
- Identity Provider (IdP)
  - Provides identity data of the subject to the service provider
  - Identification, Authentication (and Authorization)
- Relying Party (Service Provider - SP)
  - Provides services or 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

Isolated Model



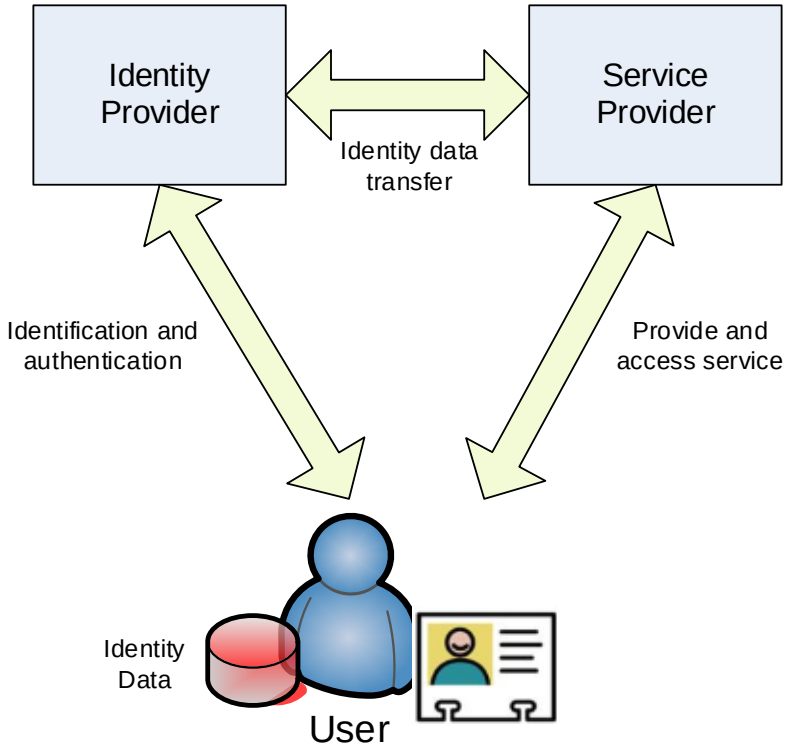
- Service Provider and Identity Provider merge
- Authentication directly at the Service Provider
- IdM system only applicable for specific Service Provider
- Identity data stored and maintained at the individual Service Provider

Central Model



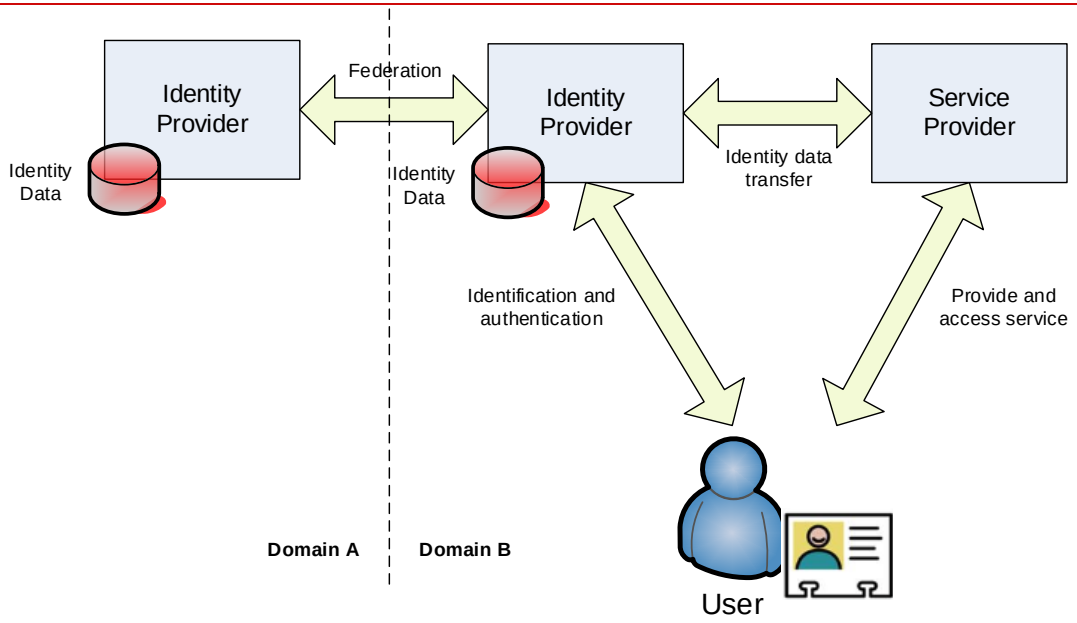
- Identity Provider (IdP) stores identity data
- IdP provides identity data to the service provider (SP)
- User has no control on actual data transfer
- e.g., Central Authentication Service (CAS), Facebook

User-Centric Model



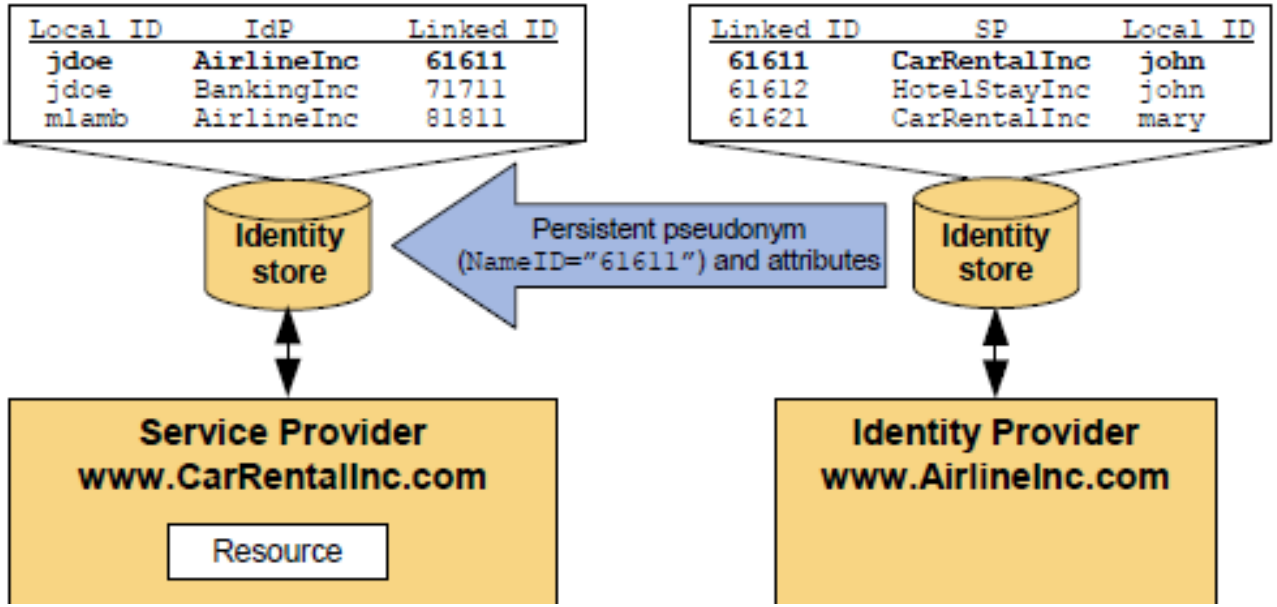
- Identity data stored in user-domain
- Usually stored on a secure token (e.g., smart card)
- Explicit user consent
- e.g., Austrian Citizen Card, German nPA

Federated Model



- Identity data distributed across several IdPs
- Trust relationship between providers required
- IdP share common identifier
- e.g., Shibboleth, WS-Federation

Identity Federation

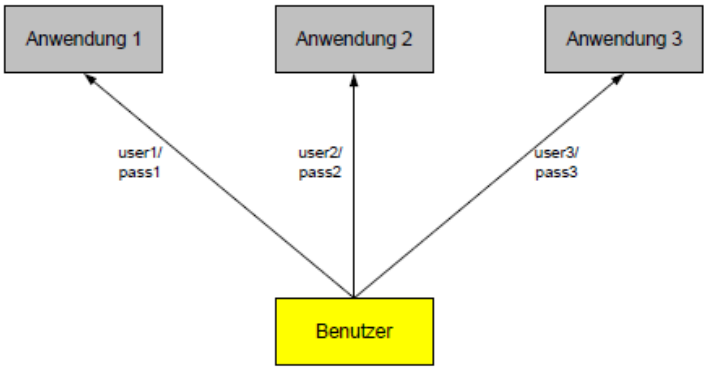


Ref: SAML 2.0 Technical Overview

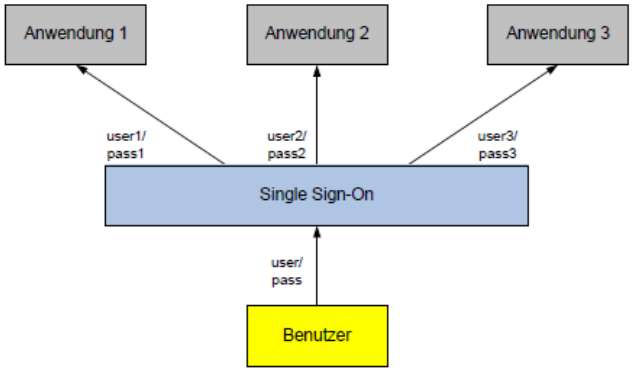
Single Sign-On (SSO)

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 – use multiple services at the same time



Normal login at multiple services



SSO-login at multiple services

Single Sign-On (SSO)

- Advantages
  - Only one authentication process
  - Prevent large number of different passwords
  - Higher level of security
  - More user comfort and efficiency
- Disadvantages
  - Central point of failure or attack
  - Key to the kingdom

Single Sign-On (SSO)

- Pseudo-SSO system
  - Local middleware storing different credentials for service providers
  - Hidden “real” authentication using the stored credentials at the service providers
  - E.g. password manager
- True-SSO system
  - Identity Provider as intermediary
  - One real authentication at the identity provider
  - Subsequent authentications at service providers based on assertions from the identity provider
  - E.g. identity protocols

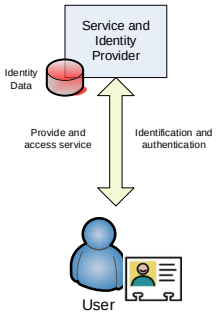
Single Logout (SLO)

- Reverse process to SSO
- Global logout at all services a user is currently logged in
- Important security feature
  - Logout at one application after SSO can lead to open authentication sessions at other applications

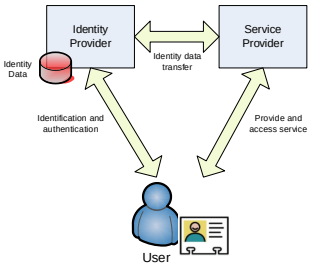
Trust Management

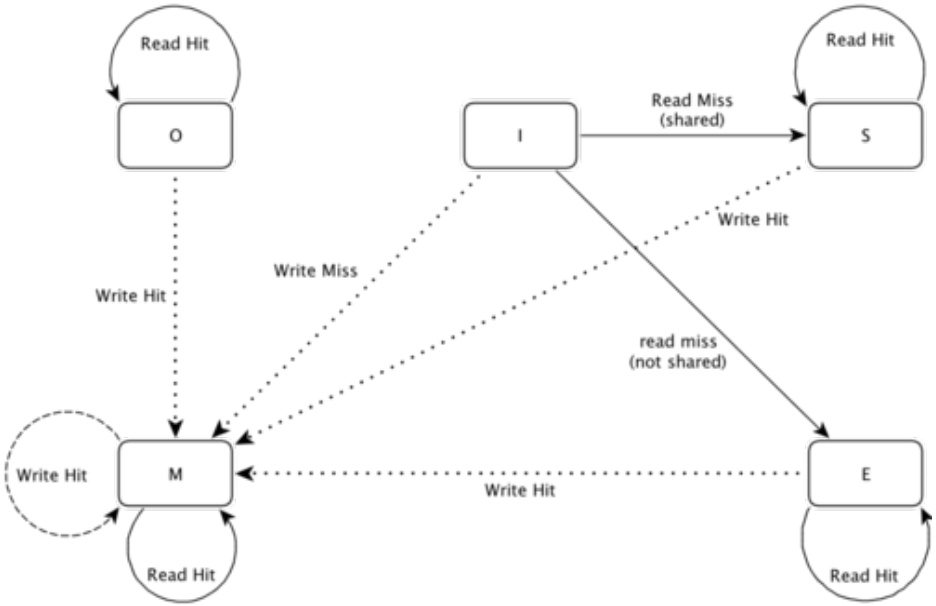
"Trust is the characteristic whereby one entity is willing to rely upon a second entity to execute a set of actions and/or to make a set of assertions about a set of principals and/or digital identities. In the general sense, trust derives from some relationship (typically a business or organizational relationship) between the entities" **[Goodner and Nadalin]**

- Direct Trust
  - One party fully trusts the other party without any intermediaries or another trusted third party



- Indirect Trust
  - Affected parties rely on claims asserted by an intermediary or a common trusted third party

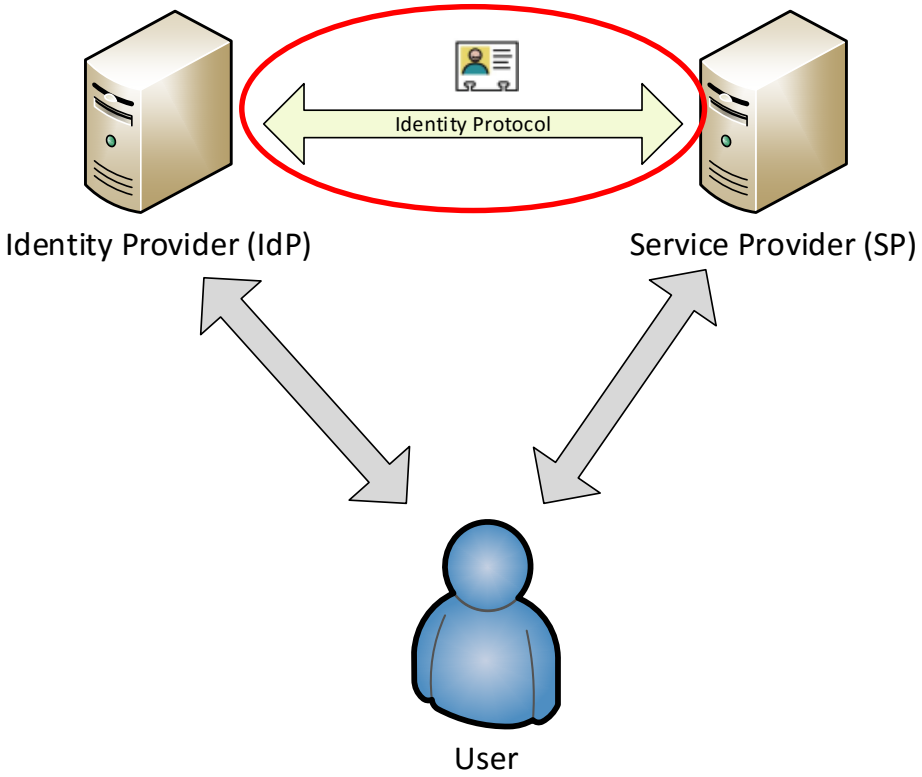




SECTION 6: PROTOCOLS

Gratitude to my colleague Bernd Zwattendorfer, who provided his lecture slides "*Selected Topics IT-Security 1*"

Identity Protocols



Identity Protocols | Terminology

Component	SAML	OAuth	OpenID Connect	CAS
Service Provider (SP)	Service Provider (Relying Party)	Client	Client	Web Service
Subject	Subject	Resource Owner	Resource Owner	User
Identity Provider (IdP)	Identity Provider	Authorization Server AND Resource Server	Authorization Server AND Resource Server	Central Authentication Server

SAML – Security Assertion Markup Language

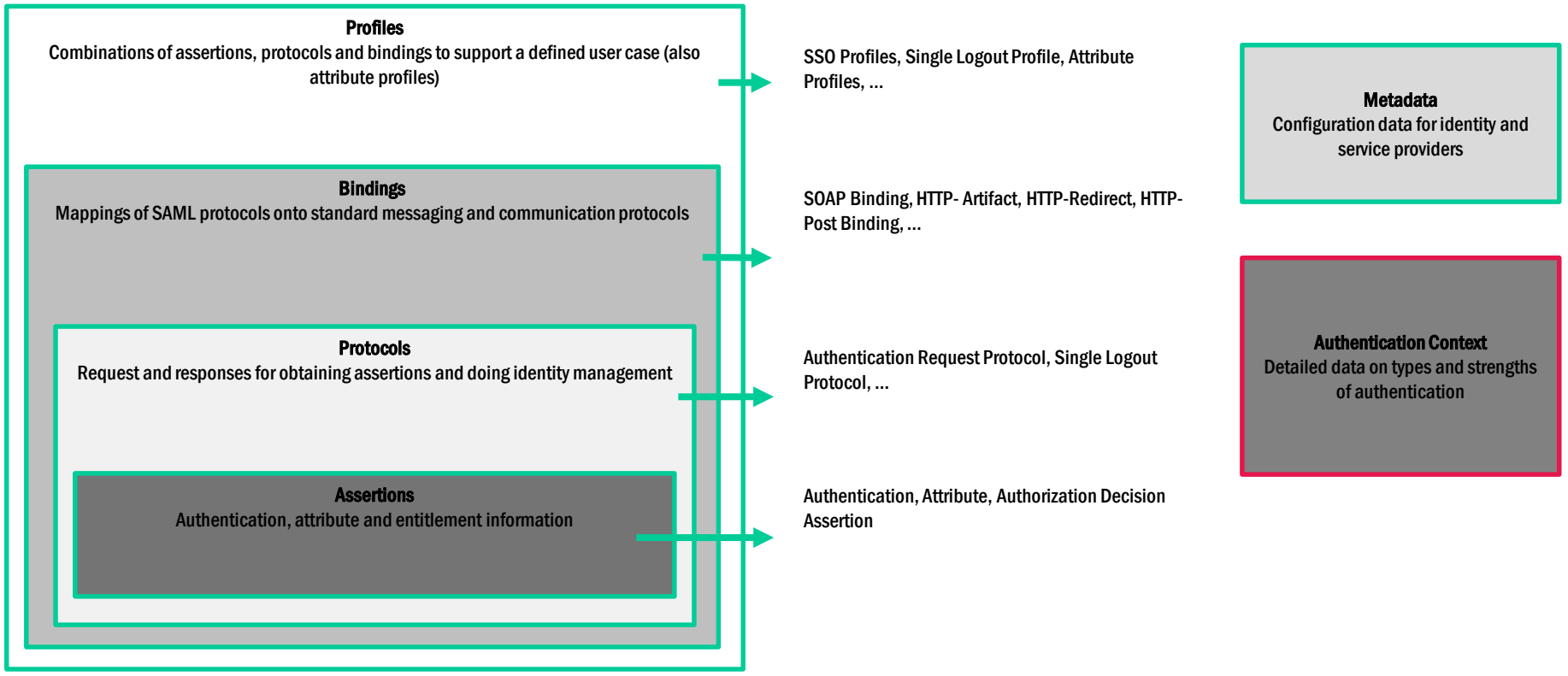
SAML | Security Assertion Markup Language

- 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
  - SAML 2.1: Currently under development
- Uses existing standards (XML-Dsig, XML-Enc, SOAP, …)
- Used within other standards (e.g. WS-Security)

SAML | Typical Use-Cases

- Web Single Sign-On (SSO)
  - Authentication at one web site and accessing multiple web sites without re-authentication (even beyond domain-borders)
- Identity federation
  - Federation of identity data across multiple systems/domains
- Attribute-based authorization
  - Authorization based on transferred attributes
- Securing Web Services
  - Transport of structured security information within other standards
- Single Logout
  - Global and simultaneous logout at multiple applications

SAML | Architecture

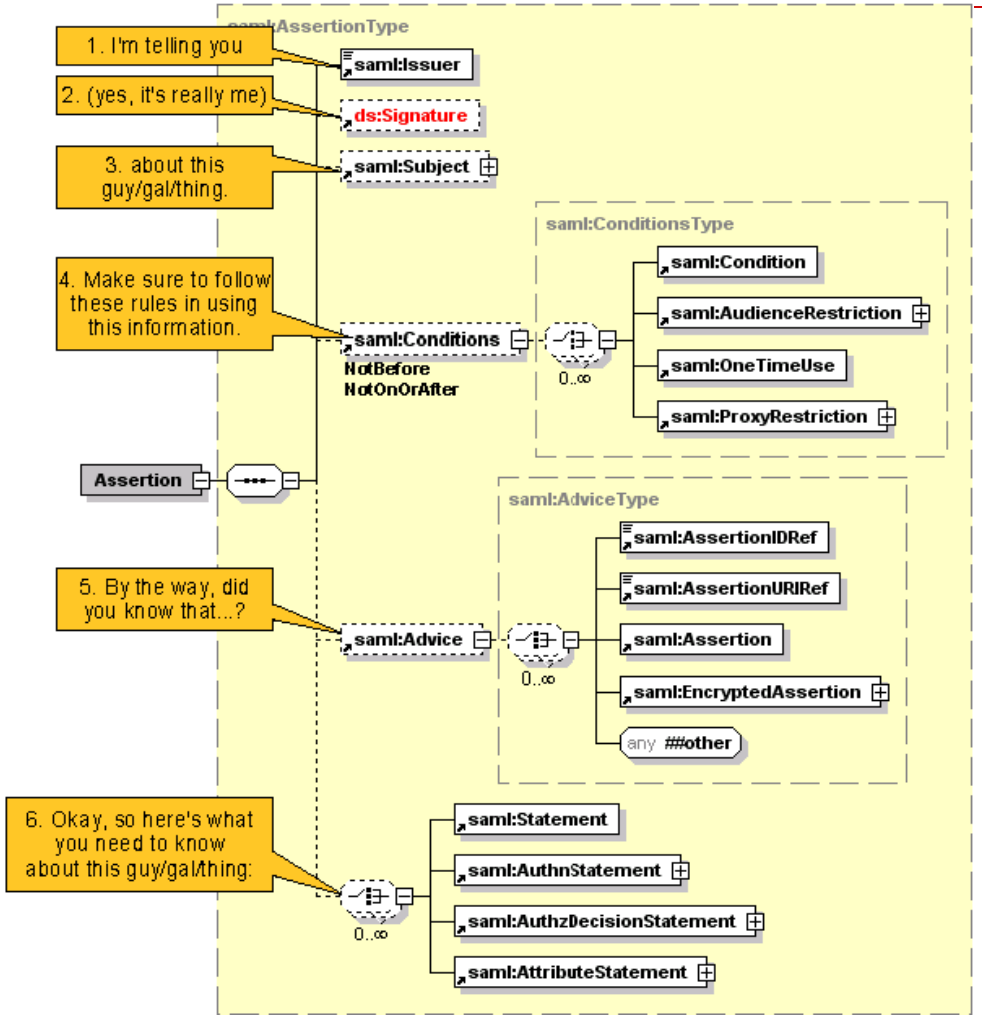


Ref: SAML 2.0 Technical Overview

SAML | Assertion

- Assertion = Claim of somebody about somebody
- SAML assertions contain different statements
  - Authentication statement
    - “Jane Doe authenticated herself on October 29, 2014 at 09:17 using a smart card.”
  - Attribute statement
    - “Jane Doe was born on January 1, 1970 and is a lawyer.”
  - Authorization statement
    - “Yes, Jane Doe is allowed to access this web site”.

SAML | Assertion



Ref: Eve Maler

SAML | Assertion Example

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  Version="2.0"
  IssueInstant="2006-07-28T14:01:00Z">
  <saml:Issuer>
    www.emeffgee.com
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
  Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
      J.Handy@emeffgee.com
    </saml:NameID>
  </saml:Subject>
  <saml:Conditions
    NotBefore="2006-07-28T14:00:05Z"
    NotOnOrAfter="2006-07-28T14:05:05Z">
  </saml:Conditions>
  <saml:AuthnStatement
    AuthnInstant="2006-07-28T14:00:05Z"
    SessionIndex="0">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute
      NameFormat="http://emeffgee.com" Name="Role" >
      <saml:AttributeValue>repair_tech</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

SAML Assertion

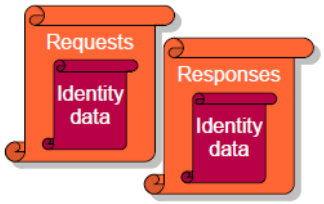
SAML Authentication Statement

SAML Attribute Statement

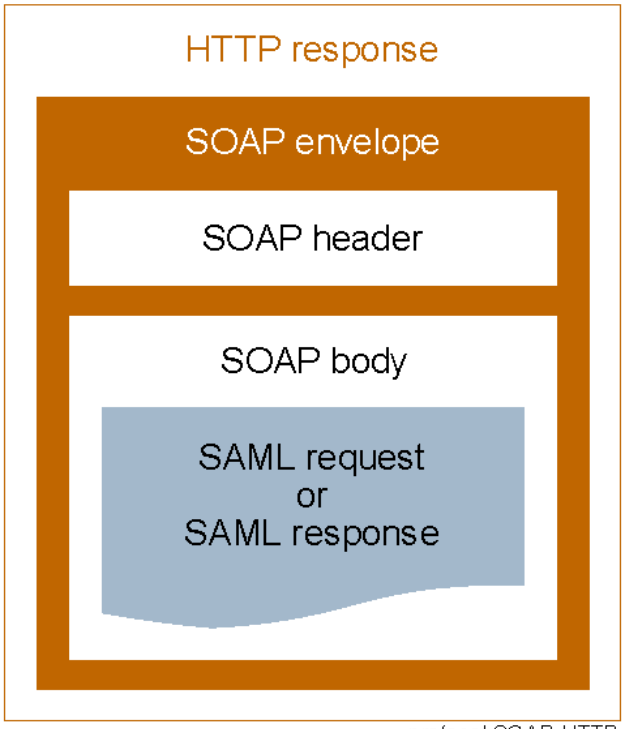
Ref: Eve Maler

SAML | Protocols

- SAML assertions are requested and are returned after successful authentication
- SAML defines different XML request/response protocols
- The messages are transferred via different communication/transportation protocols (SAML Bindings)



SAML | Bindings (Example: SAML via SOAP over HTTP)



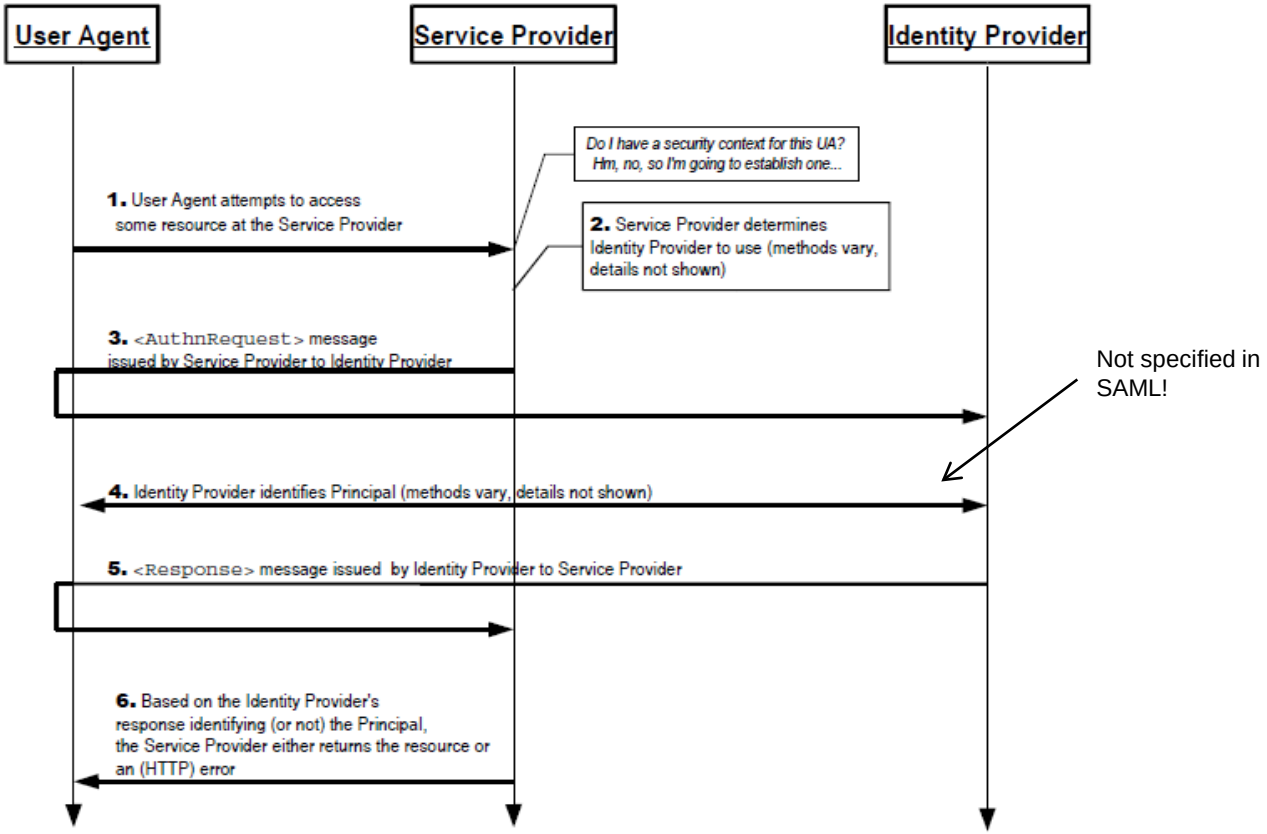
protocol-SOAP-HTTP

```
1.  <?xml version="1.0" encoding="UTF-8"?>
2.  <env:Envelope
3.    xmlns:env="http://www.w3.org/2003/05/soap/envelope/">
4.    <env:Body>
5.      <samlp:AttributeQuery
6.        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
7.        xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
8.        ID="aaf23196-1773-2113-474a-fe114412ab72"
9.        Version="2.0"
10.       IssueInstant="2006-07-17T20:31:40Z">
11.       <saml:Issuer>http://example.sp.com</saml:Issuer>
12.       <saml:Subject>
13.           <saml:NameID
14.           Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
15.           C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
16.           </saml:NameID>
17.       </saml:Subject>
18.       <saml:Attribute
19.           NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
20.           Name="urn:oid:2.5.4.42"
21.           FriendlyName="givenName">
22.       </saml:Attribute>
23.     </samlp:AttributeQuery>
24.   </env:Body>
25. </env:Envelope>
```

SAML | Profiles

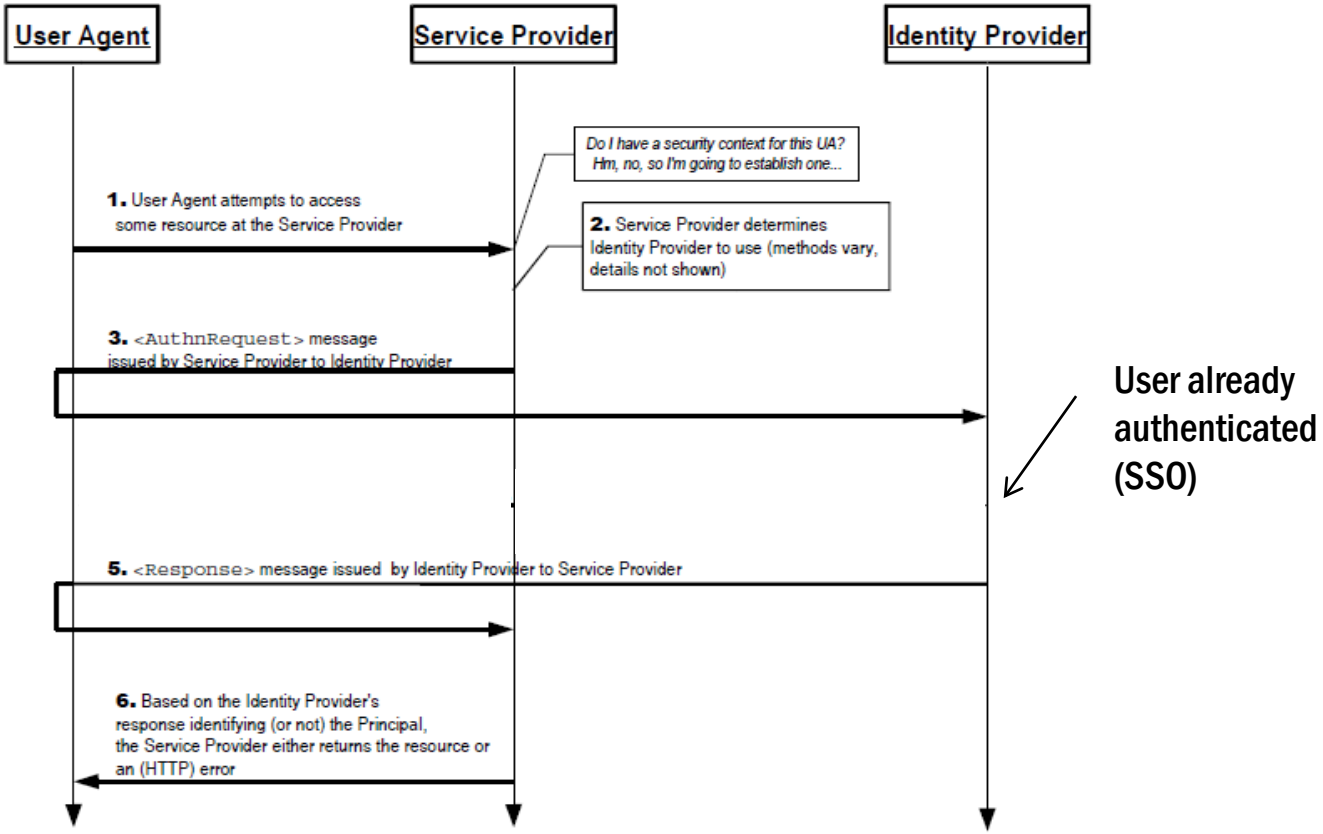
- Model the SAML use cases by combining SAML Assertions, SAML Protocols and SAML Bindings
  - Single sign-on, identity federation, single logout, …
- Profiles are standardized but own profiles may be created
  - E.g. Kantara, STORK, eIDAS specification, …

SAML | Login Process



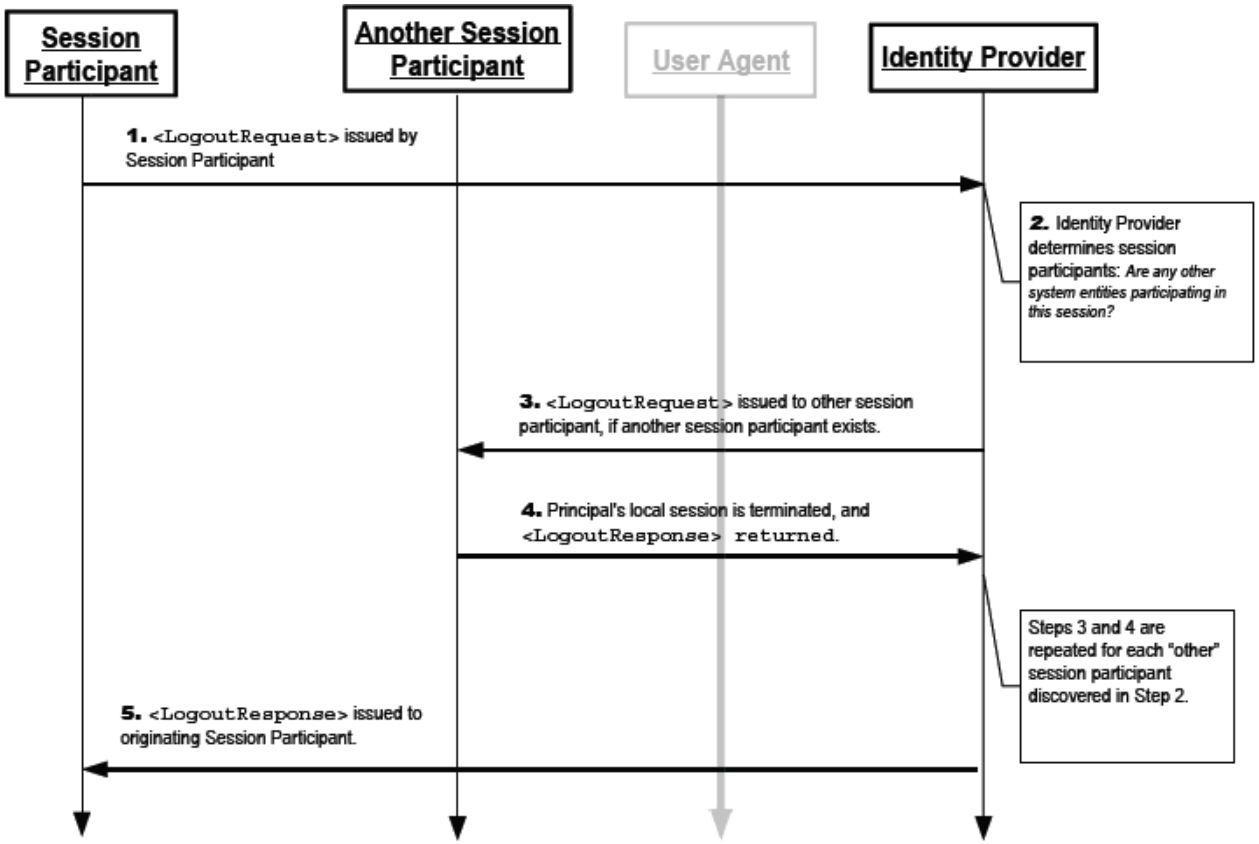
Ref: SAML 2.0 Core

SAML | SSO Login Process



Ref: SAML 2.0 Core

SAML | Single Logout Process



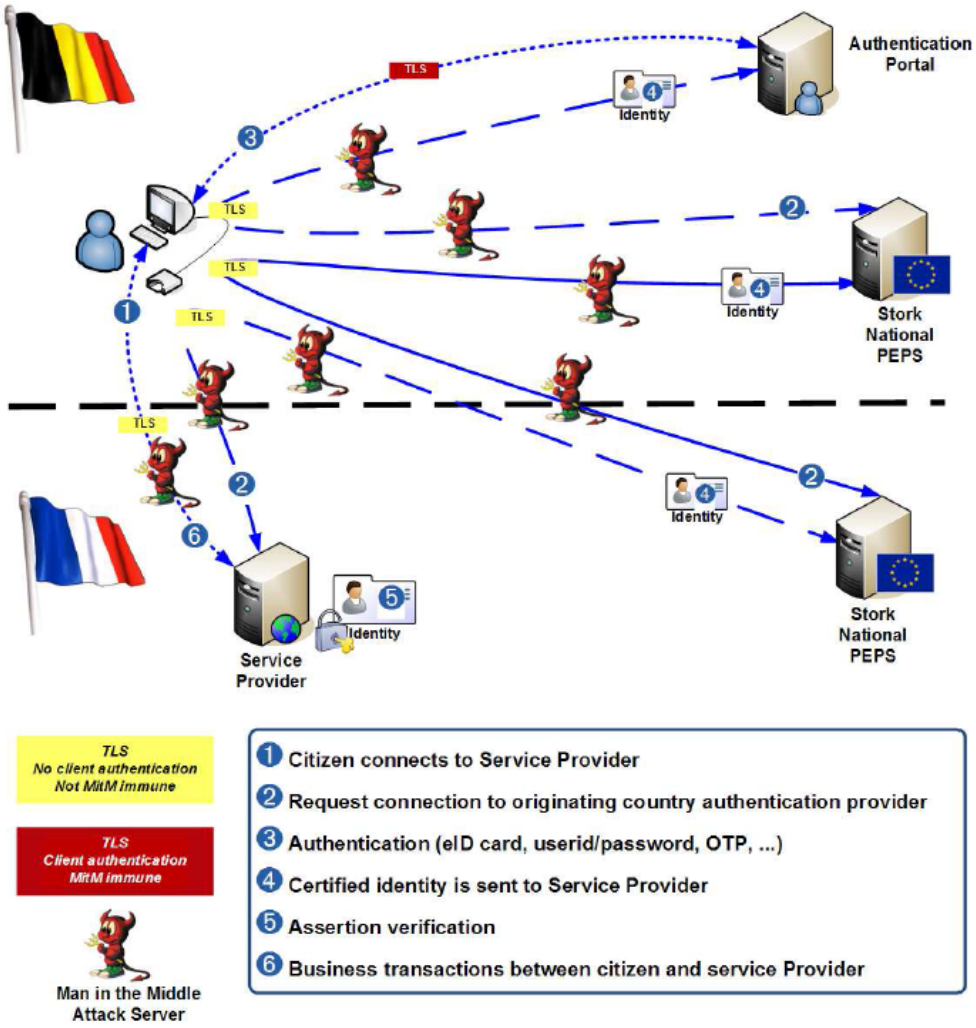
Ref: SAML 2.0 Core

SAML Holder-of-key (HoK) Profile

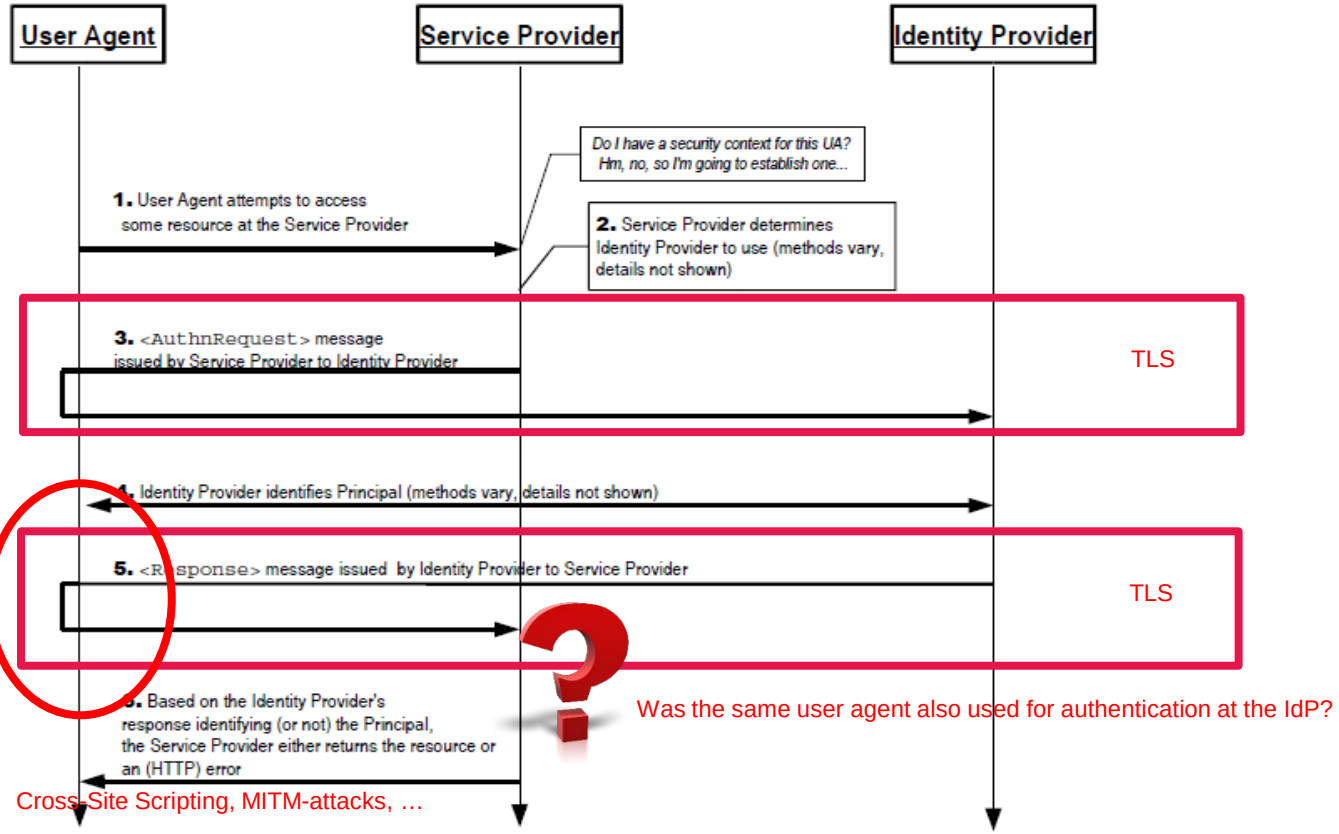
- Enhance the security of SAML message exchange without requiring modifications to client software
- Stronger security context between IdP and SP
- Use of underlying TLS session and X.509 certificates
- Cryptographic binding between SAML assertion and user agent due to the use of TLS client certificates (can be self-signed!)
- Stolen assertions are useless for an attacker since he does not posses the private key for TLS authentication

Holder-of-key: what is it good for?

- A preview to STORK …

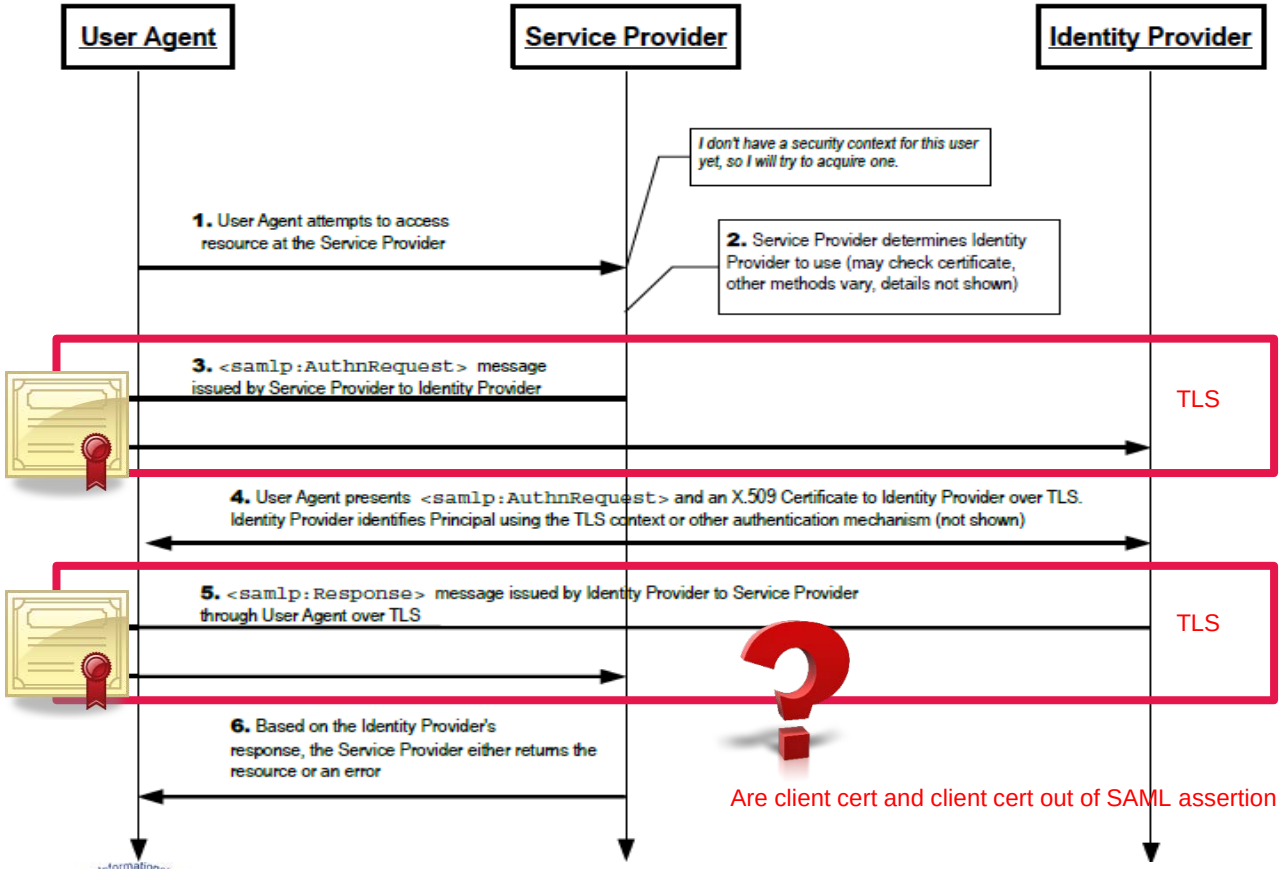


SAML | Standard Login Process



Ref: SAML 2.0 Core

SAML | HoK Login Process



Client cert is included into signed SAML assertion

Are client cert and client cert out of SAML assertion equal?

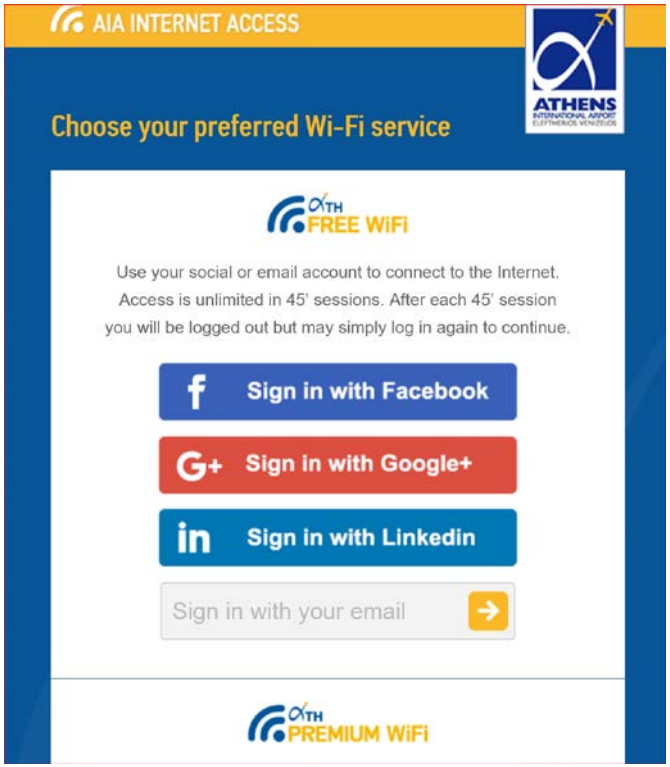
Ref: SAML 2.0 HoK

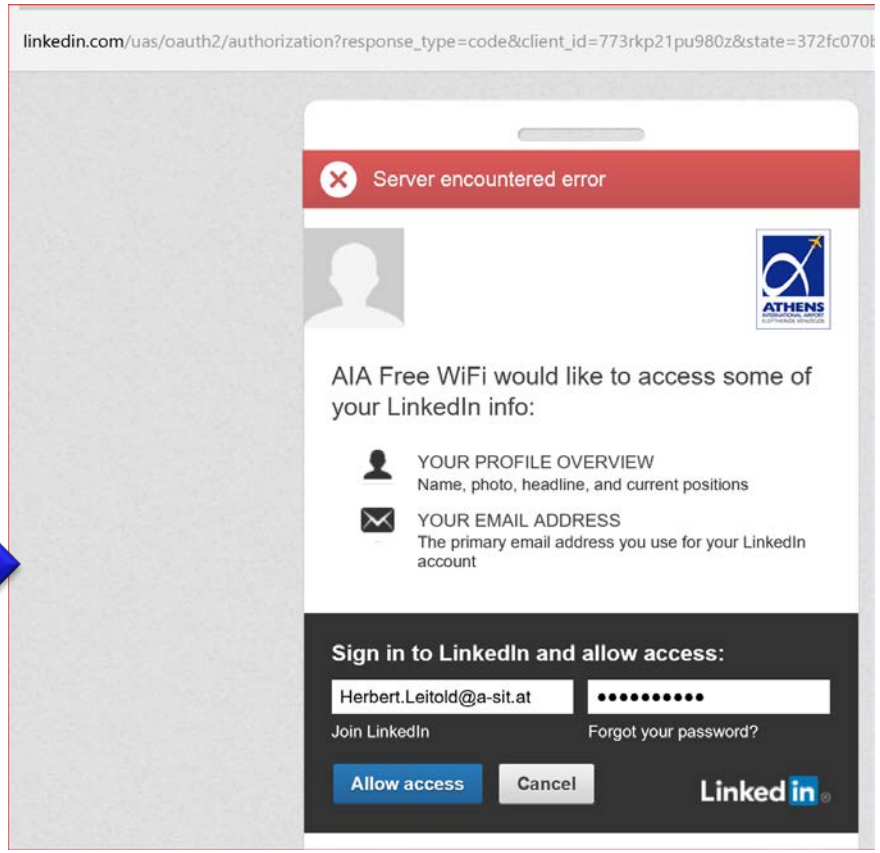
OAuth 2

OAuth

- Authorization protocol for desktop-, web- and mobile applications
- Allows applications to access a user's resources
- Users don't have to forward credentials to the application
- Established standard
  - Version 1.0: 2010
  - Version 2.0 2012

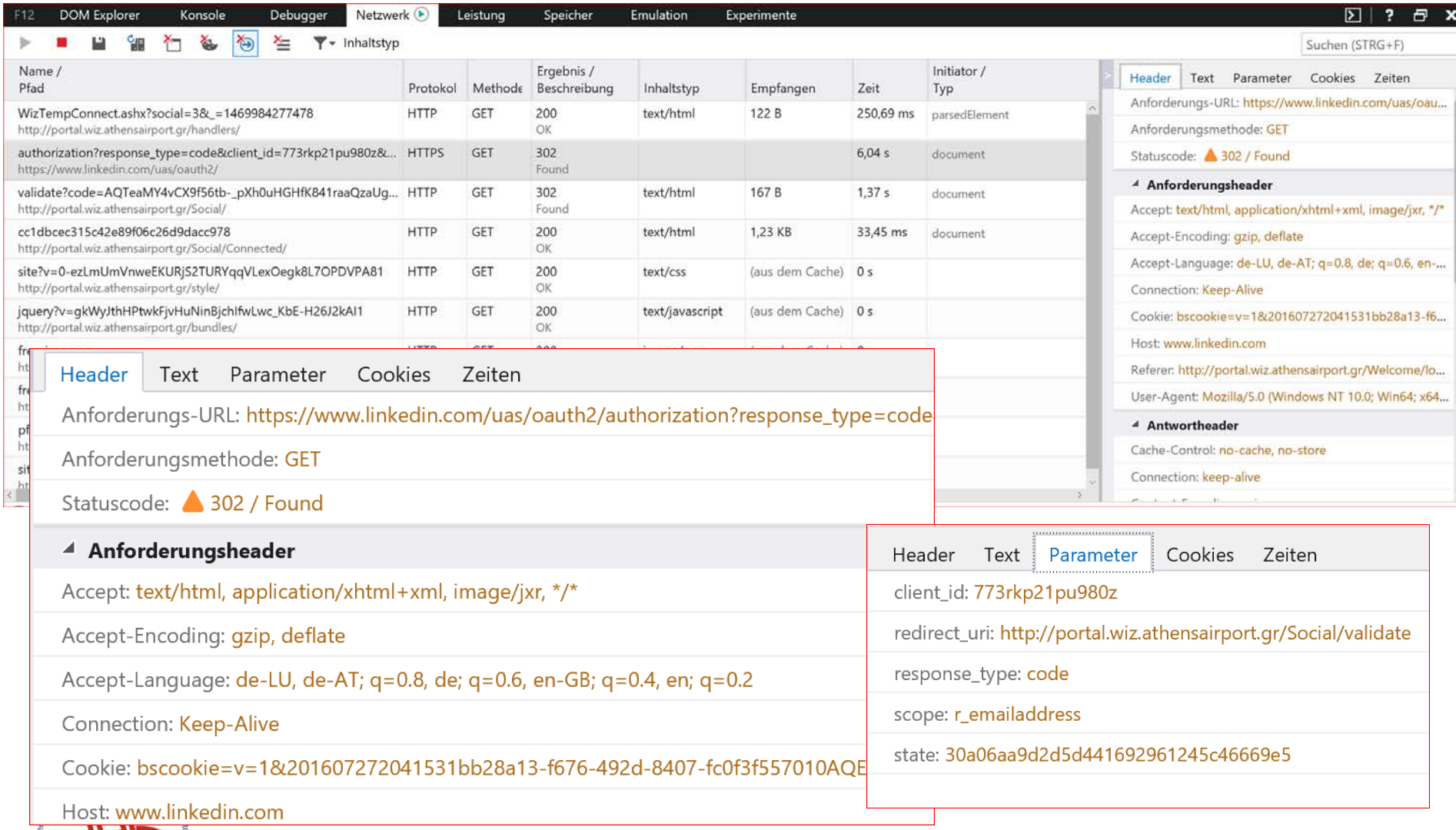
An example: Athens airport this Sunday



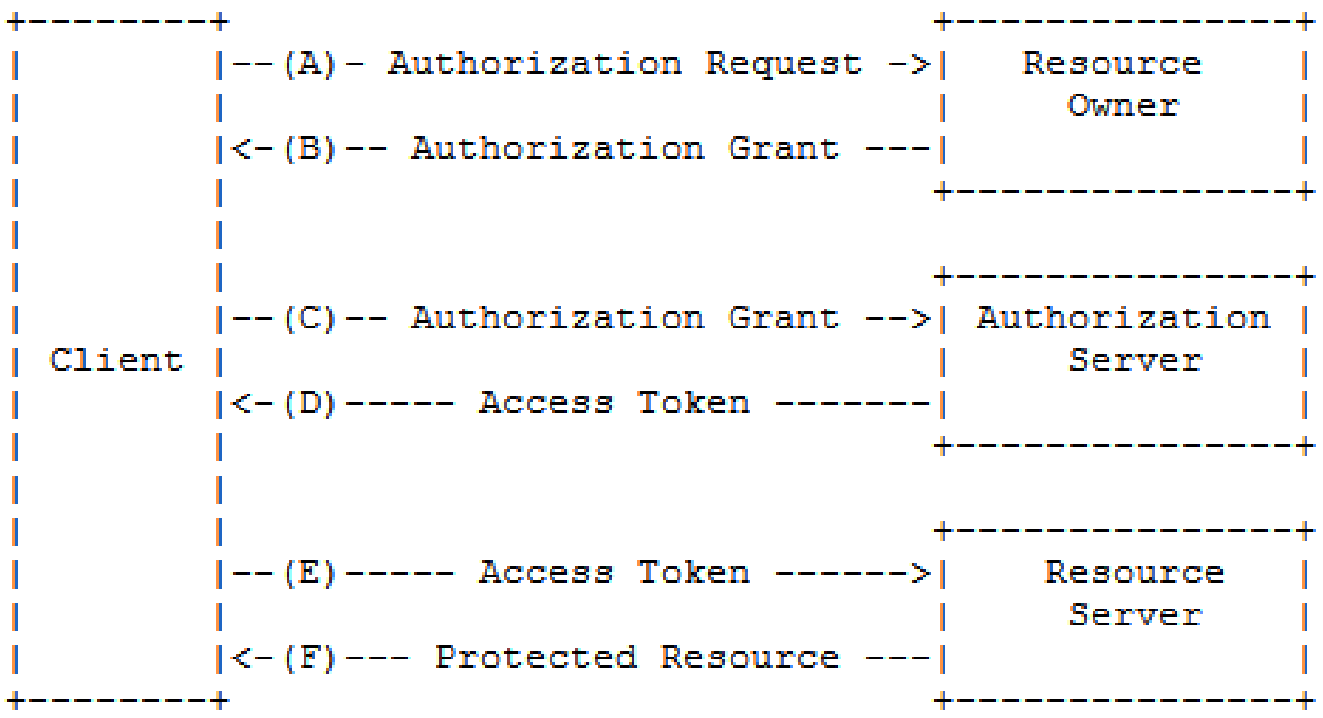


linkedin.com/uas/oauth2/authorization?response_type=code&client_id=773rkp21pu980z&state=372fc070b2c804e669ba5663659cec3fd&scope=r_emailaddress&redirect_uri=http://portal.wiz.athensairport.gr/Social/validate

Example Ahens airport ctd.



OAuth | Process Flow



Client ... Service Provider

Resource Owner ... User

Authorization Server ... Handles authentication of the user and authorization of the client

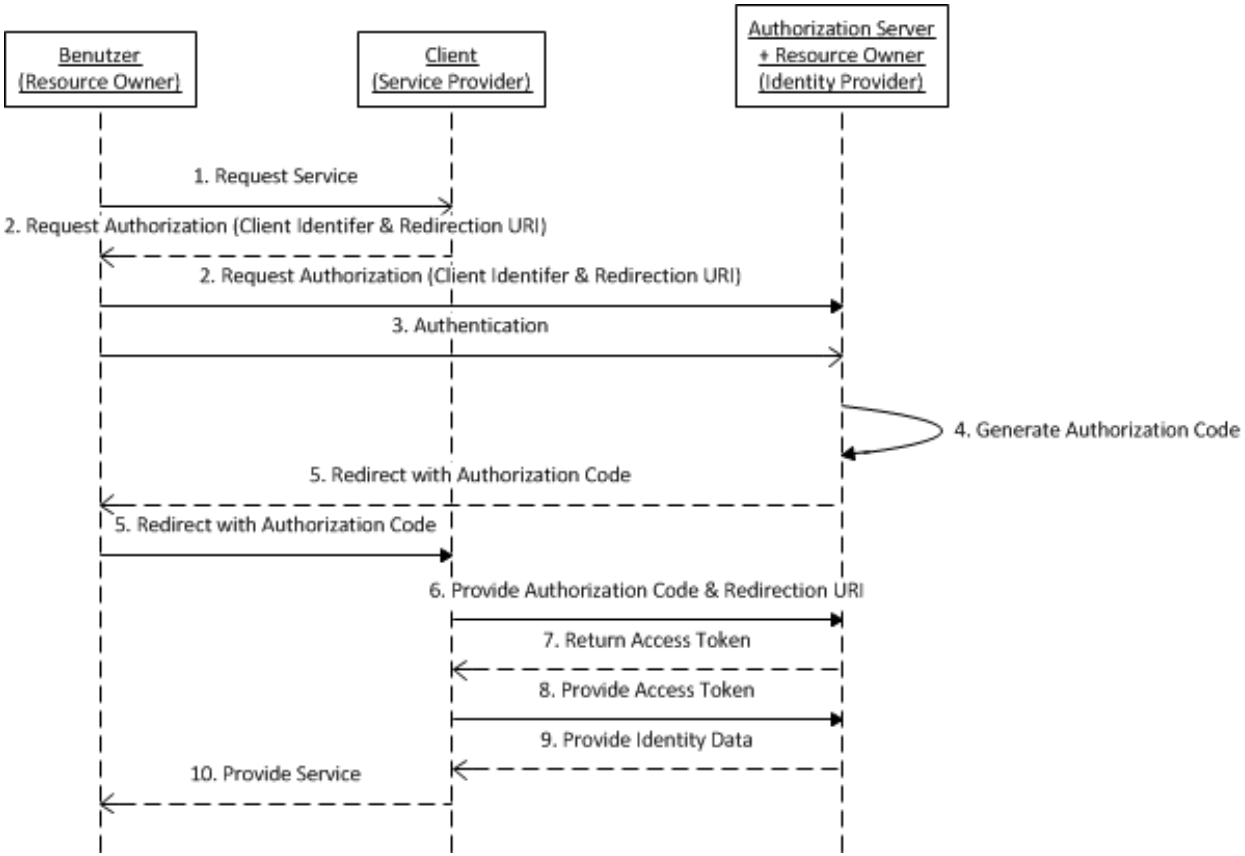
Resource Server ... Server that hosts the protected resource

Ref: RFC 6749

OpenID Connect

- Identification and authentication layer based on OAuth 2.0
- Authentication instead of authorization
- OpenID Connect protocol has nothing in common with the OpenID protocol (deprecated)
- No XML, only URL parameters or JSON
- Standard (version 1.0) since February 2014

OpenID Connect | Process Flow



OpenID Connect | Messages

```
GET /userinfo HTTP/1.1
Host: moa-id.gv.at
Authorization: Bearer SIAV32hkKG
```

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
"sub":"12345==",
"given_name":"Max",
"family_name":,"Mustermann"
"birthdate":,"01-01-1990"
"gender":,"M"
}
```

- UserInfo request
- UserInfo response

Difference between SAML and OpenID Connect

SAML

OpenID Connect

» **Authentication Request**

```
<saml2p:AuthnRequest xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
    AssertionConsumerServiceIndex="1" AttributeConsumingServiceIndex="0"
    Destination="https://demo.egiz.gv.at/demoportal_moaid-2.0/pvp2/post"
    ID="_e1ecdd2d80062991f8f0f489dfc49441" 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-sso/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="#_e1ecdd2d80062991f8f0f489dfc49441">
                <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>qGqkR6stEnKFS04DQ6yx44CDzzo=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
<ds:SignatureValue>GhvpD+urP2BwEaejBW3Y3dmdIKdFDR9AikVn0TAyWBg3d/+gYxBQ0JHPn/XCoHP6QQHbNHjfqf8o2wJQrvX9WD/BPJHK2wwecbzPK2cC1coSbGqhGq+LKwHPesHu10nr1fj4T8IAHX4lPiYR5OEDM
XtV1SvHfW1zXEBGh/MyJtk2qAFDT4OfgIneNk8hYPjcwNbBMwMME+tIR97snFMzkXI5tHSKB8LzGIPq+K2A0c06AX2LJiT8xaDscJTqqeaub4zIm6haZ1LZX0qMH2jFJVfjAfYbV2BhdSs6aseTLSp+k2rlPJqvpds8PBN26I8KYb
k/bwQIZ0frSSo//f+q2cw==</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:KeyValue>
                <ds:RSAKeyValue>
<ds:Modulus>nEPzKMh3TovnfBnTyv+TMYFsGep8UiI7iNbfVyfLoBfqRdeGDOk4es2qWkgB6az+kM/9Js2H06m4
pjEY7/RIJd0IMWqgi8eqdjiiMmbFQykkYYQhIZbvi8KqoBcCKzj5N3GY4qh8A5qN4y8SQ3sZj23T
iiIY1rphE+ZTOHCm6CKeRso9jj409YHP1xAXfPvt1Yx2TA1uuagxOmL750C/hr7gcUmOtmuKiSeq
+TO4VZwZQ7K7YESZ1WkiBoG2i4cHdcBFKnVrGNtyxi6UkjWxXRJSU9aNLs5QxsE6iFwCvFoIO+IU
cWWxFfHqOGbRtAcRUb4fk+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-sso/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>
```

```
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
```

Difference between SAML and OpenID Connect

SAML

- Authentication Response

OpenID Connect

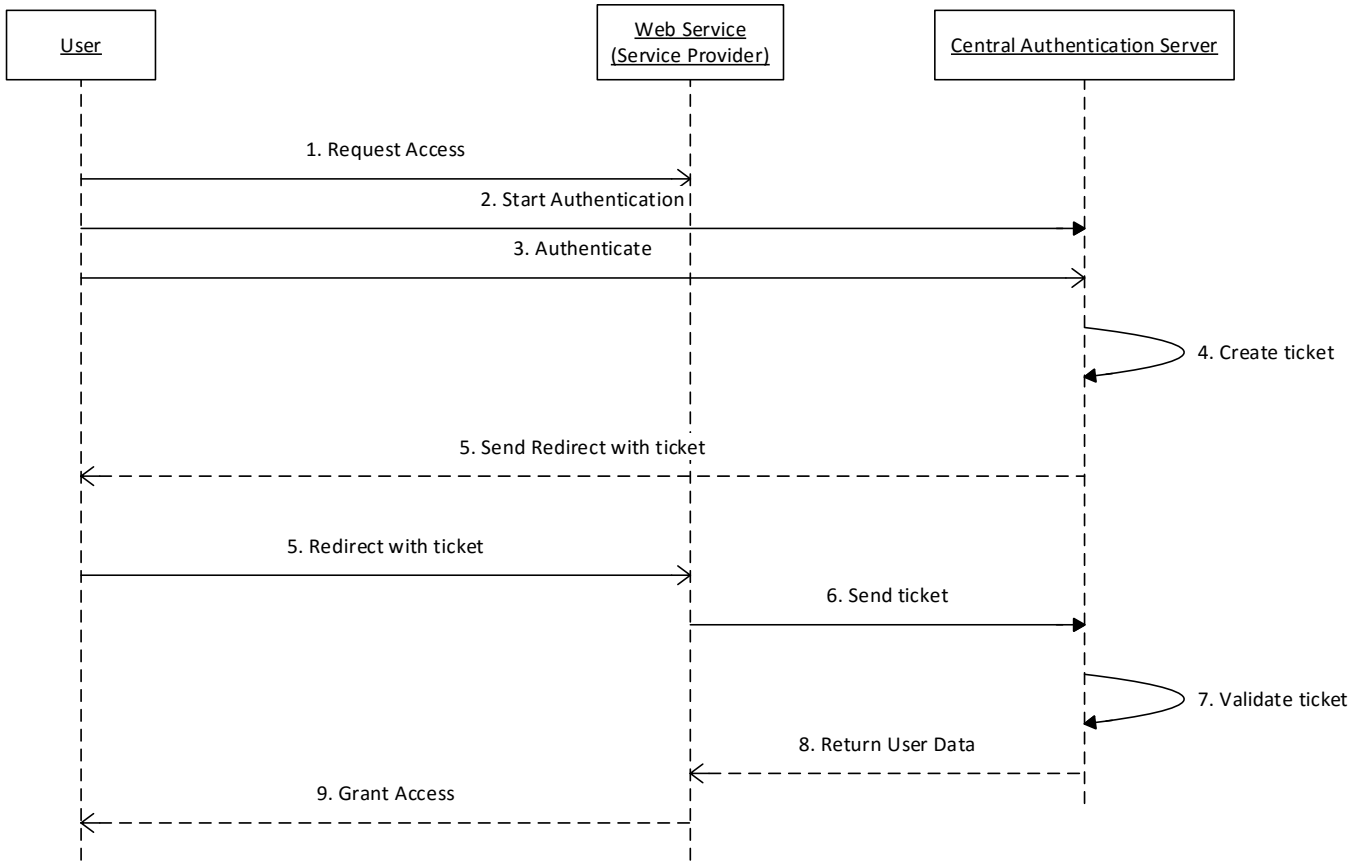
```
HTTP/1.1 200 OK
Content-Type:
application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
"sub":"12345==",
"given_name":"Max",
"family_name":,"Mustermann"
"birthdate":,"01-01-1990"
"gender":,"M"
}
```

CAS – Central Authentication Service

Central Authentication Service (CAS)

- Central open-source SSO solution
  - CAS server written in Java
  - Multiple client libraries (Java, PHP, etc.)
- History
  - Initiated by the University of Yale in 2001
  - Since 2005 a project of Jasig (Java Architectures Special Interest Group)
- Mostly URL parameters, since Version 3.0 parts in XML
- Version 1.0: 2001
- Version 2.0: 2002
  - Added proxy authentication
- Version 3.0: 2014
  - New architecture based on plug-ins
  - Further protocols: CAS 1,2,3; SAML 1.1, OpenID, OAuth 1.0,2.0
  - Added XML Messages

CAS | Process Flow



CAS | Messages

- **Authentication Request (/login)**

```
https://cas.example.org/cas/login?service=http%3A%2F%2Fwww.example.org%2Fservice
```

- **Redirect with Ticket (/validate)**

```
https://cas.example.org/cas/validate?service=http%3A%2F%2Fwww.example.org%2Fservice&ticket=ST-1856339-aA5Yuvrxzpv8Tau1cYQ7
```

- **Authentication Response**

CAS 1.0

```
Yes
username
```

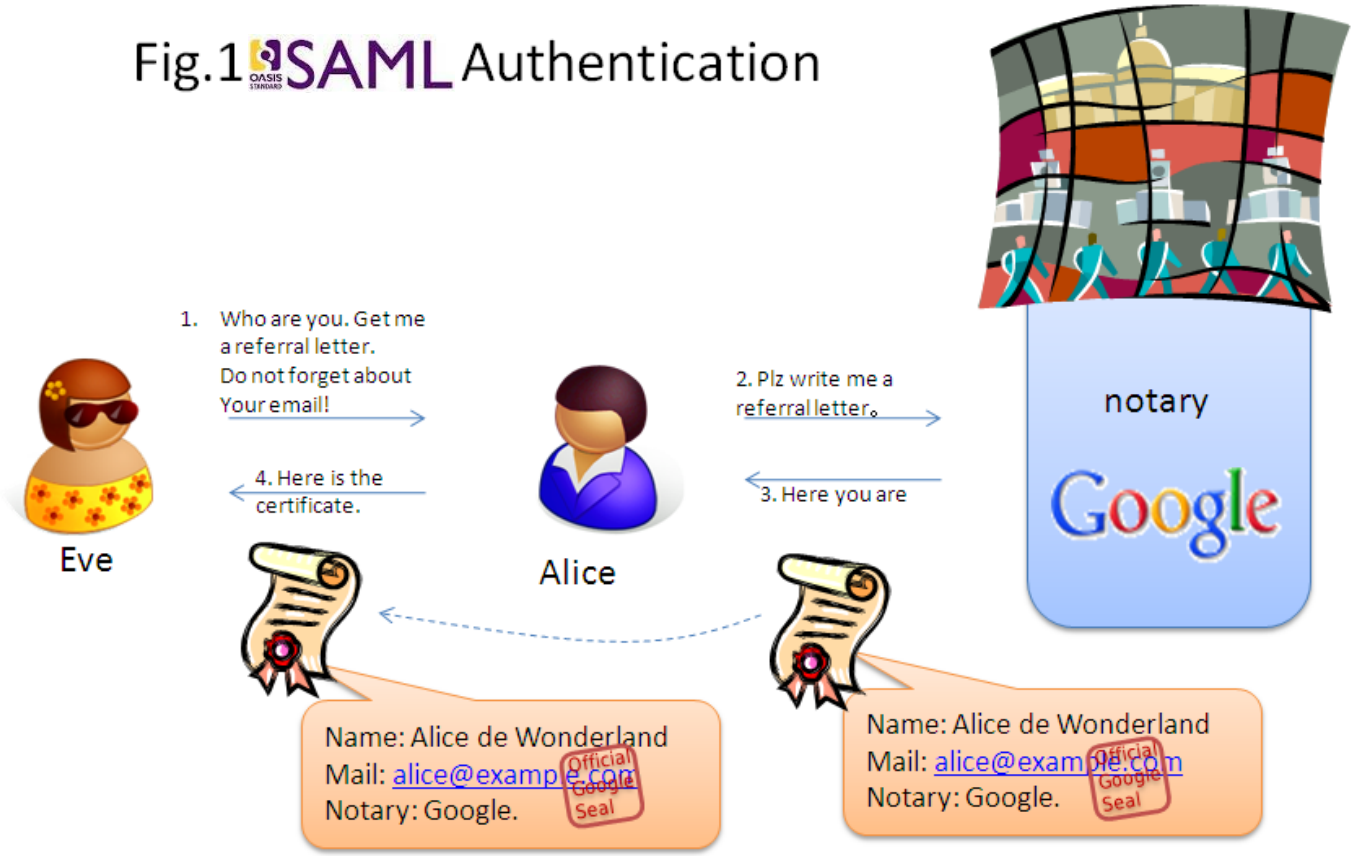
CAS 3.0

```
<cas:serviceResponse
xmlns:cas="http://www.yale.edu/tp/cas">
 <cas:authenticationSuccess>
  <cas:user>username</cas:user>
  <cas:proxyGrantingTicket>PGTIOU-84678-
8a9d...</cas:proxyGrantingTicket>
 </cas:authenticationSuccess>
</cas:serviceResponse>
```

Identity Provider

- Google, Facebook, Twitter
  - SSO using these accounts
  - Different identity providers and identity protocols
    - SAML, OpenID, OpenID Connect

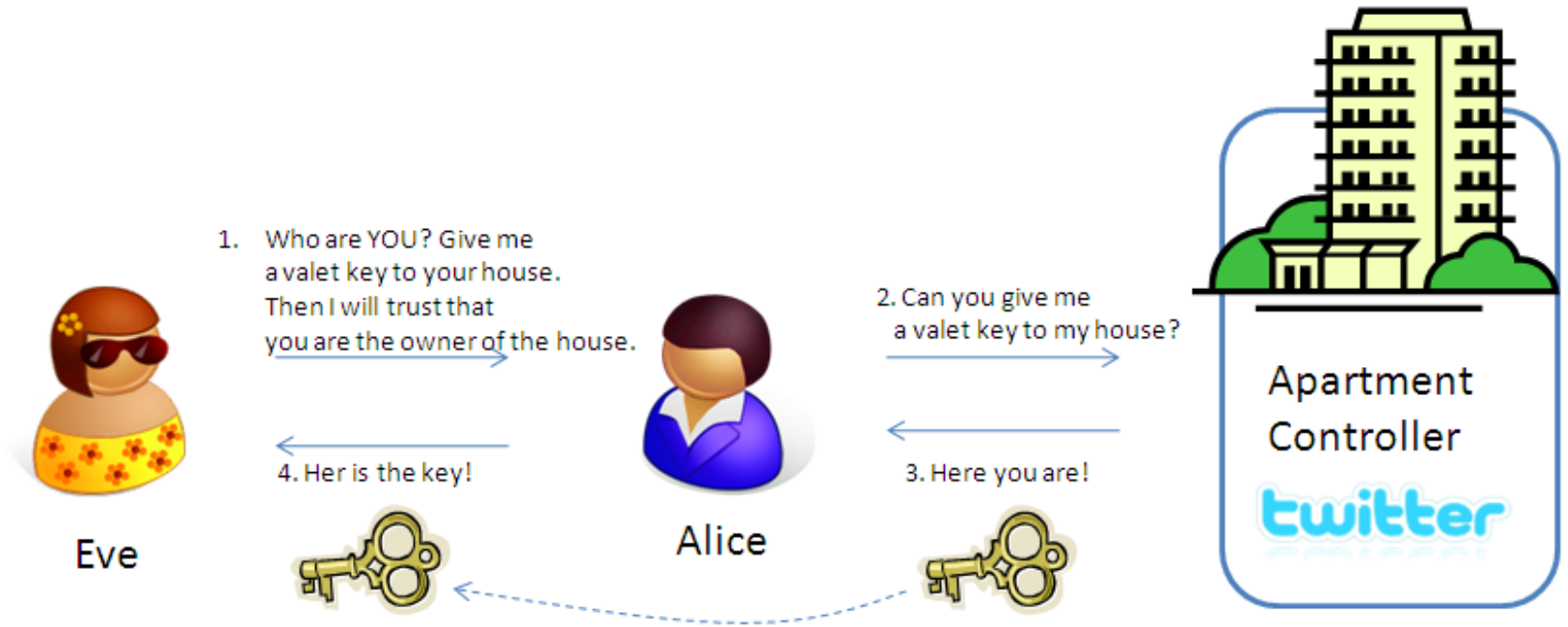
Summary



Ref:
Sakimura

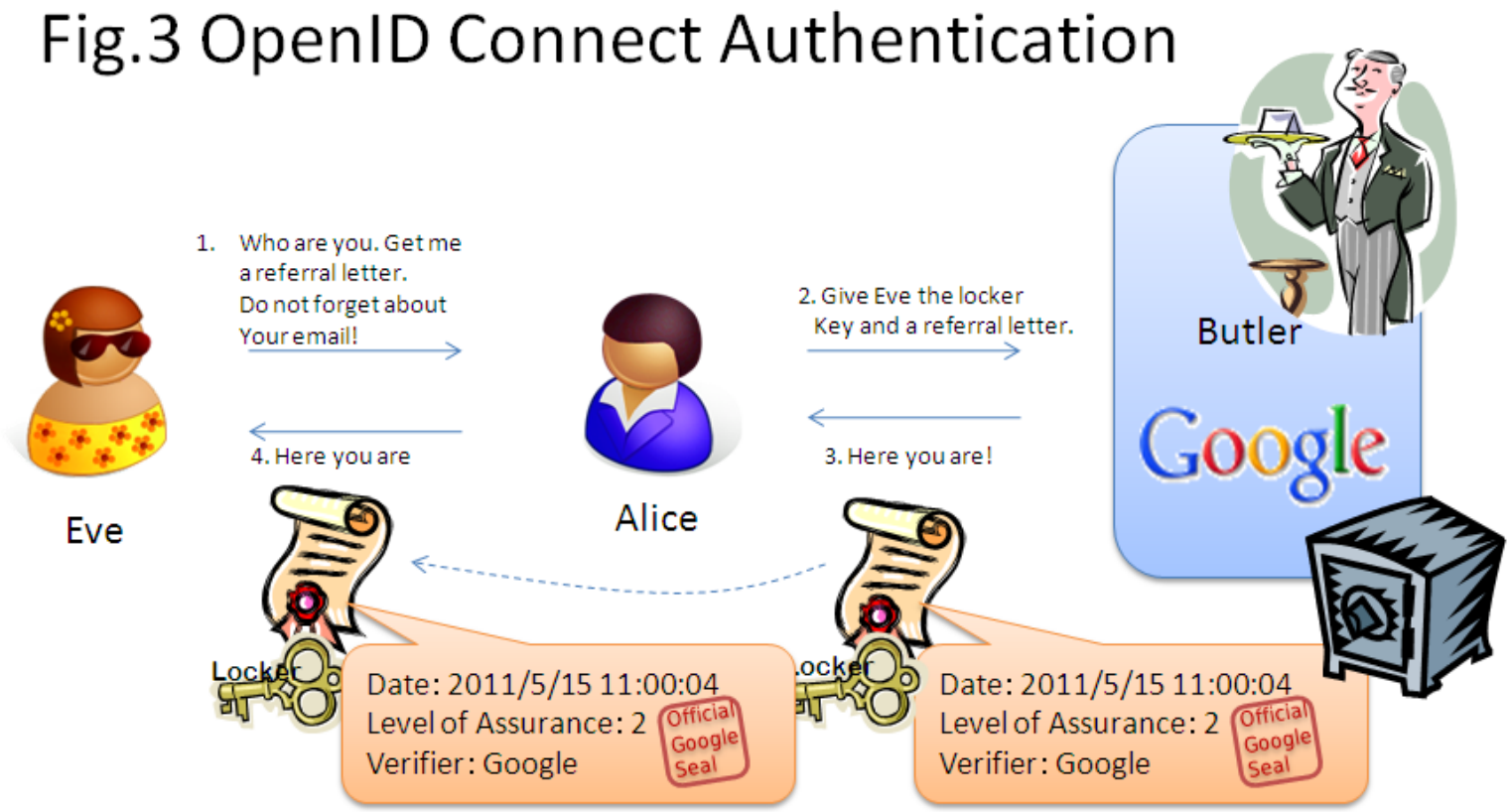
Summary

Fig.2 Pseudo-Authentication using OAuth



Ref:
Sakimura

Summary



Ref: Sakimura