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 …

UNINETT FEIDE

KALMAR2

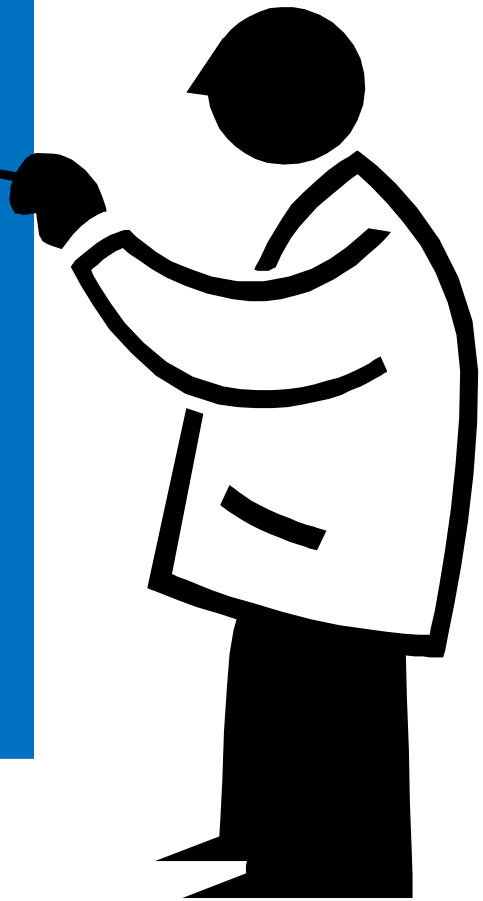
ID-porten

  - 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

Claim 1: There is a case for quality (e)ID

see e.g. „How to Steal An Identity
https://www.youtube.com/watch?v=-URDjwb0fS4

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

Evolved as national islands

- 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

Starting Point: National eIDs

- Heterogeneous in various dimensions
  - Technology
    - o Smartcards: AT, BE, DE, EE, ES, FI, IT, PT, SE, …..
    - o Mobile eID: AT, EE, FI, LU, NL, NO, UK, …
    - o Soft certif.: ES, SE, SI, …
    - o usern./pass.: NL, UK, …
    - … STORK operated on some 100+ tokens
  - Operational
    - o Issued by public sector, private sector, combined
    - o Issued at federal, local, regional level
    - o Use of identifiers
  - Legal
    - o (limited) use of identifiers; flat, sectoral, combined
    - o (lacking) mutual recognition

Starting Point: National eIDs

- Heterogeneous in various dimensions
  - Technology
    - o Smartcards: AT, BE, DE, EE, ES, FI, IT, PT, SE, …..
    - o Mobile eID: AT, EE, FI, LU, NL, NO, UK, …
    - o Smartcertif.: ES, SE, SI, …
    - o user/pass.: All, UK, …
    - o STORK operates with some 100+ tokens
  - Operational
    - o Issued by public sector, private sector, combined
    - o Issued at federal, regional level
    - o Use of identifiers
  - Legal
    - o (limited) use of identifiers; flat, sectoral, combined
    - o (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?

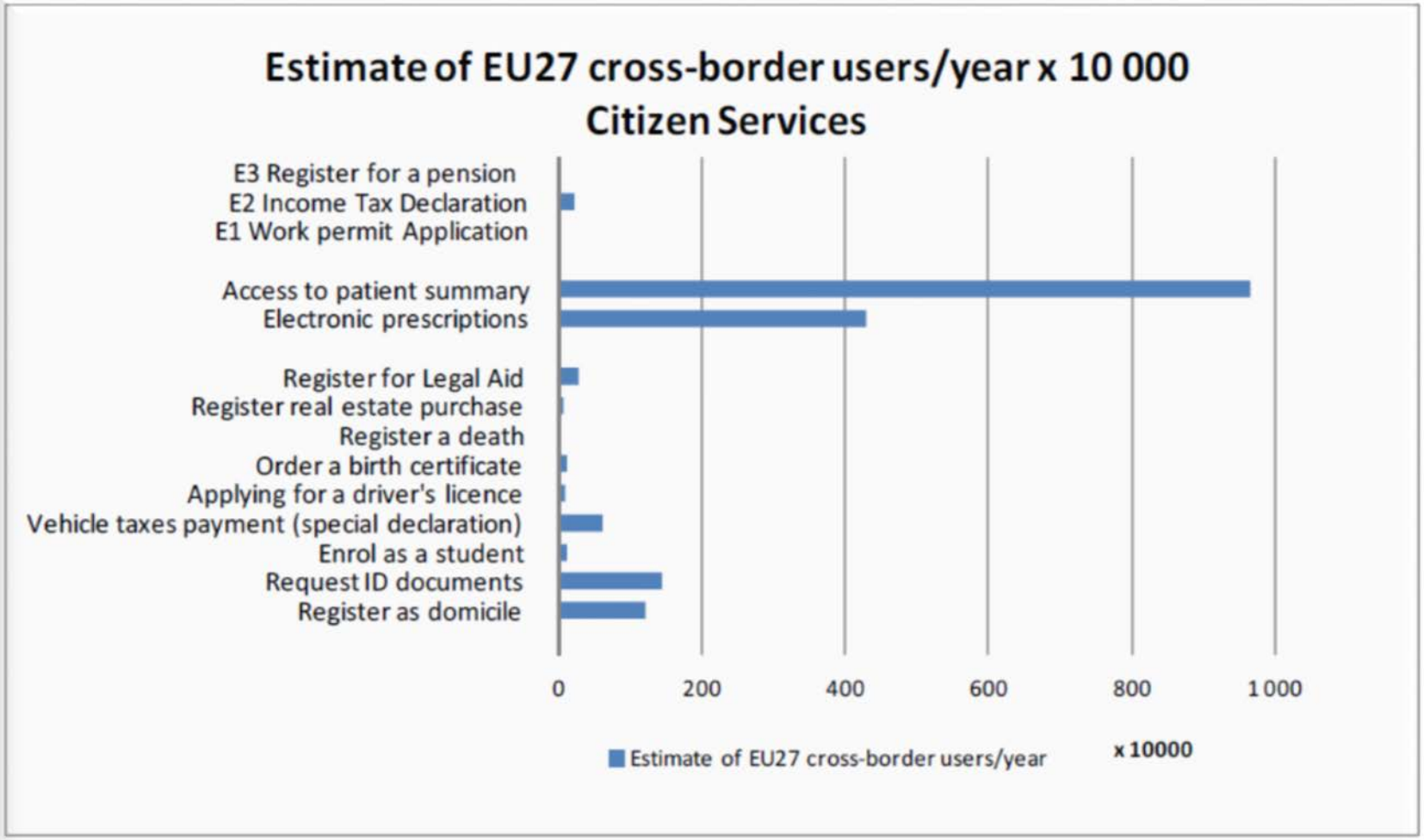


Figure 4 Estimate of EU27 cross-border users per year: citizen services

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

Need of cross-border business services?

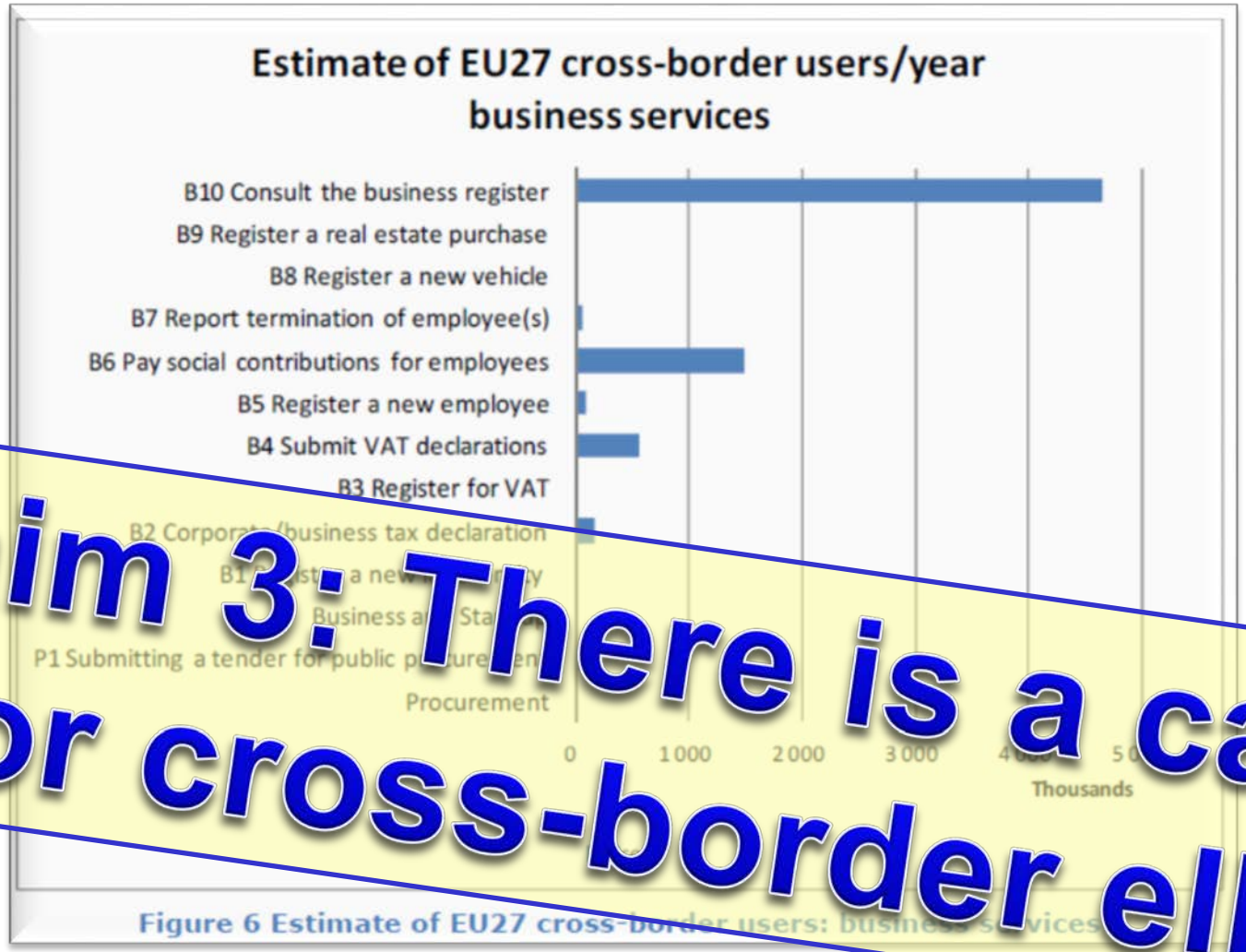


Figure 6 Estimate of EU27 cross-border users: business services

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

ADAPTING THE INFRASTRUCTURE

eGovernment eID and Authentication

2006 | 2007 | 2008 | 2009 | 2010

EU provisions: Recognition of national eIDs

Federated eID Management

Authentication Model & Levels

Common eID Framework

Equal Treatment of national eIDs

eID Terminology

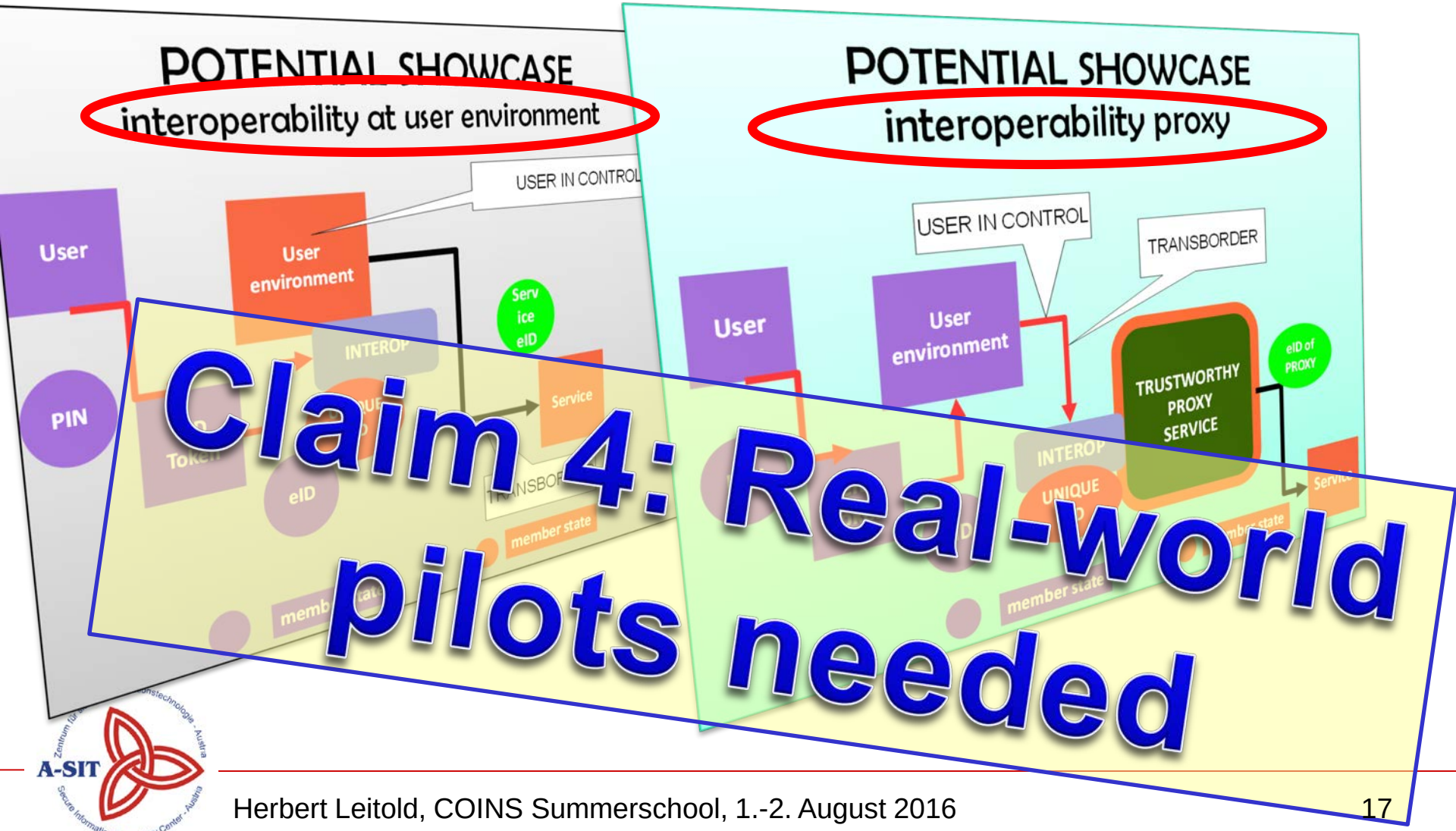
Definition of eID

eID Role Management

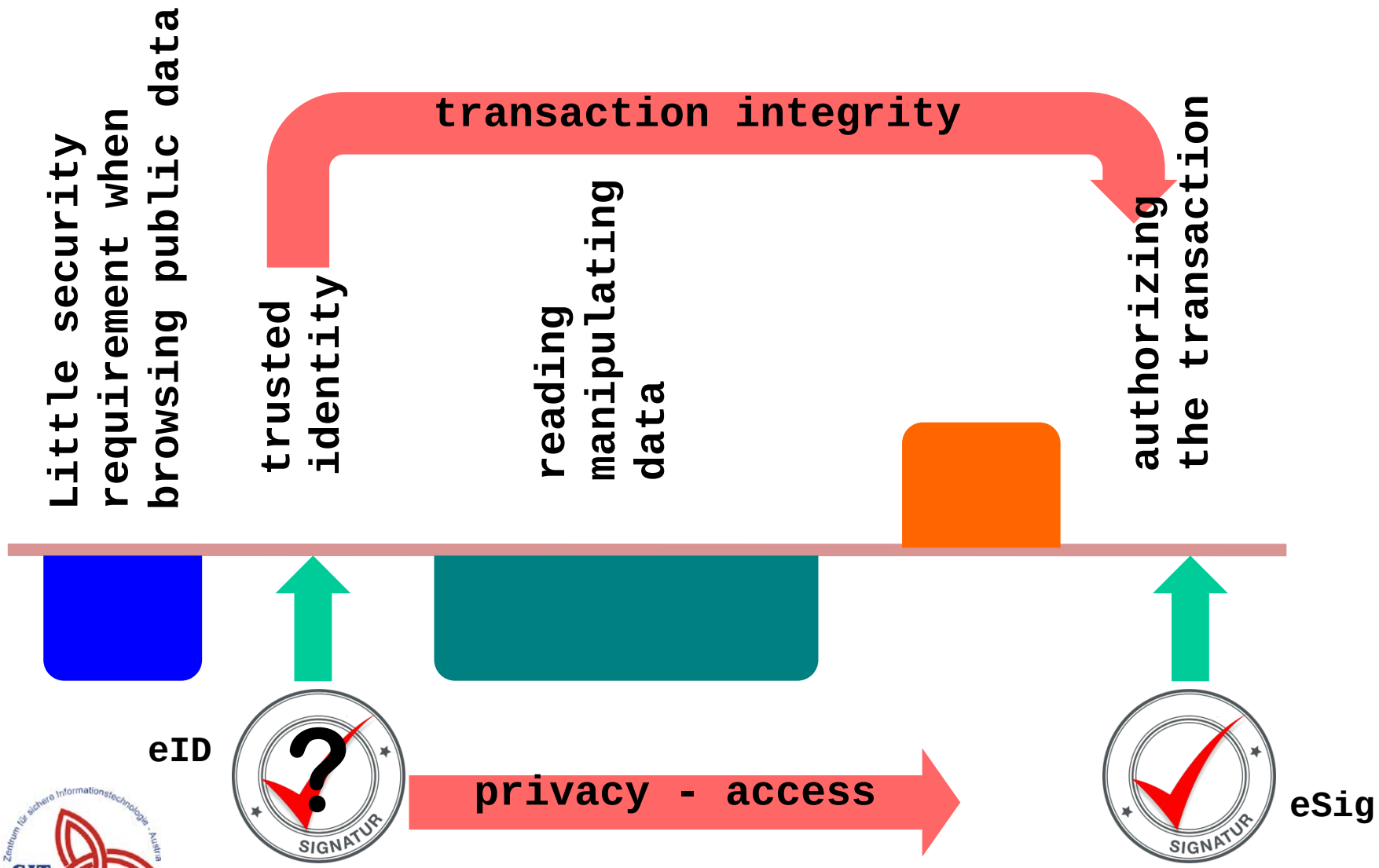
Personal Data Ownership Model

A little history: eID ad hoc-group

(2004-2005)

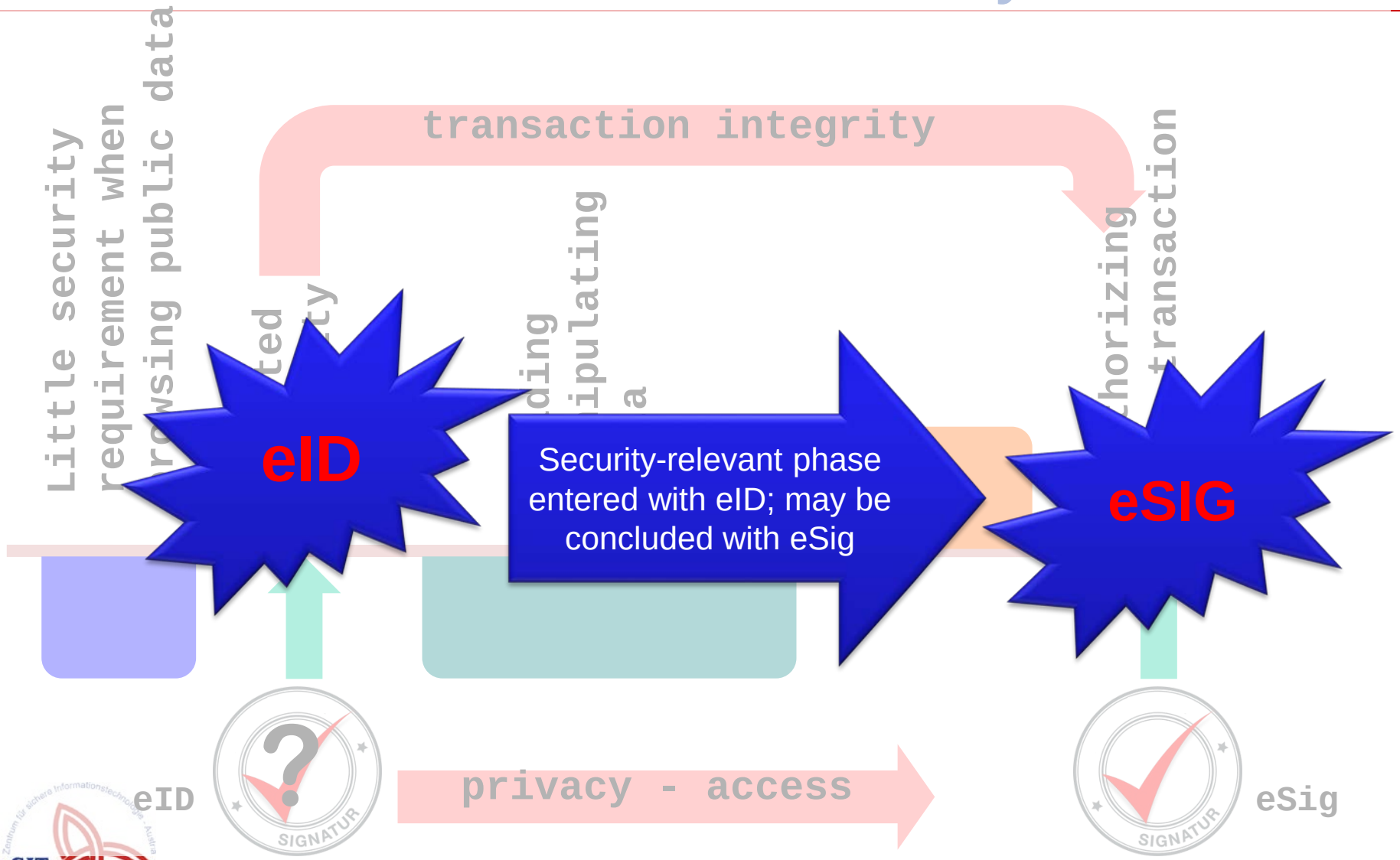


Citizen transaction and security



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

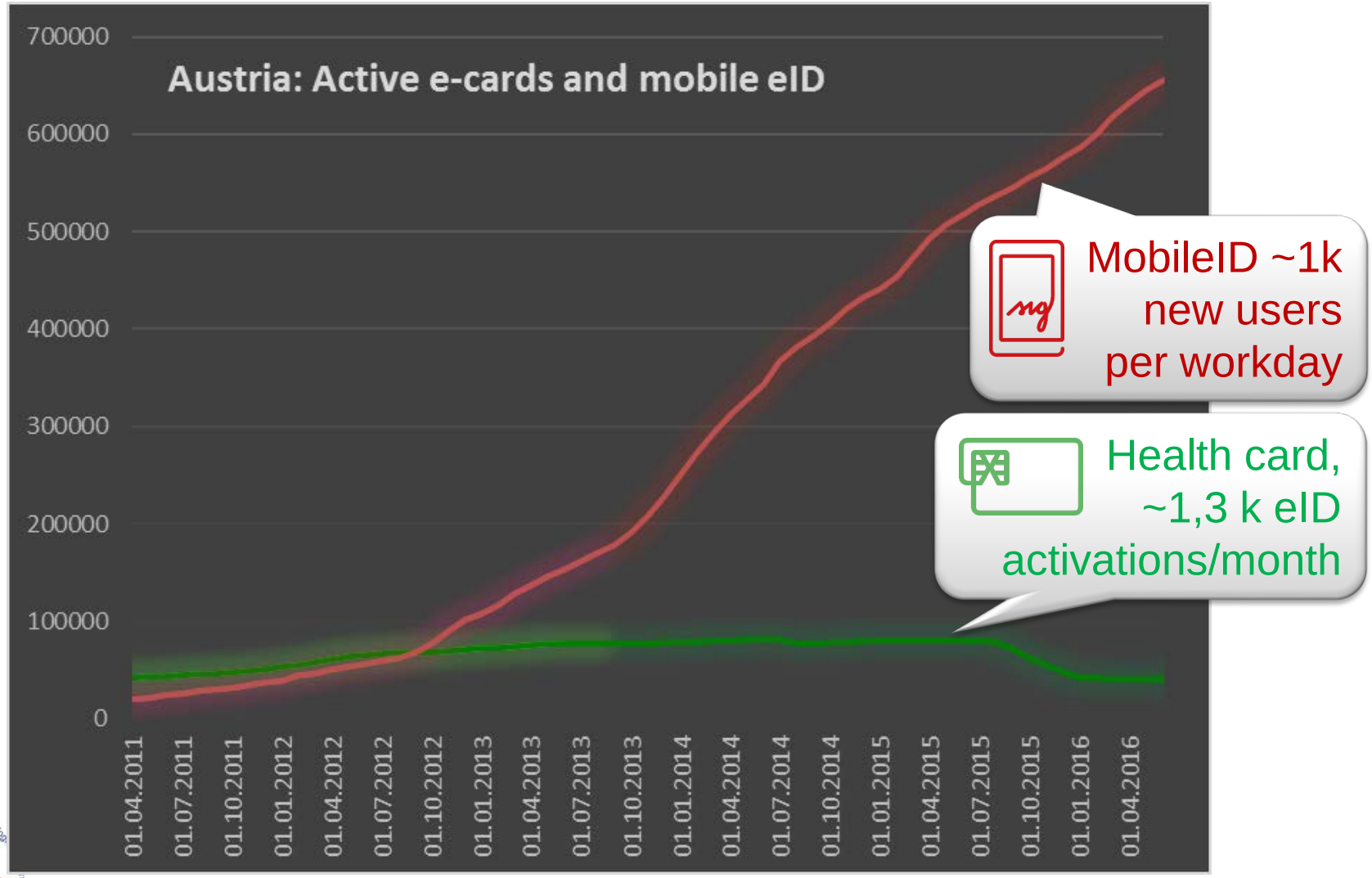
Profession cards, service cards, …
e.g. notaries, lawyers, ministries, …

Mobile

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

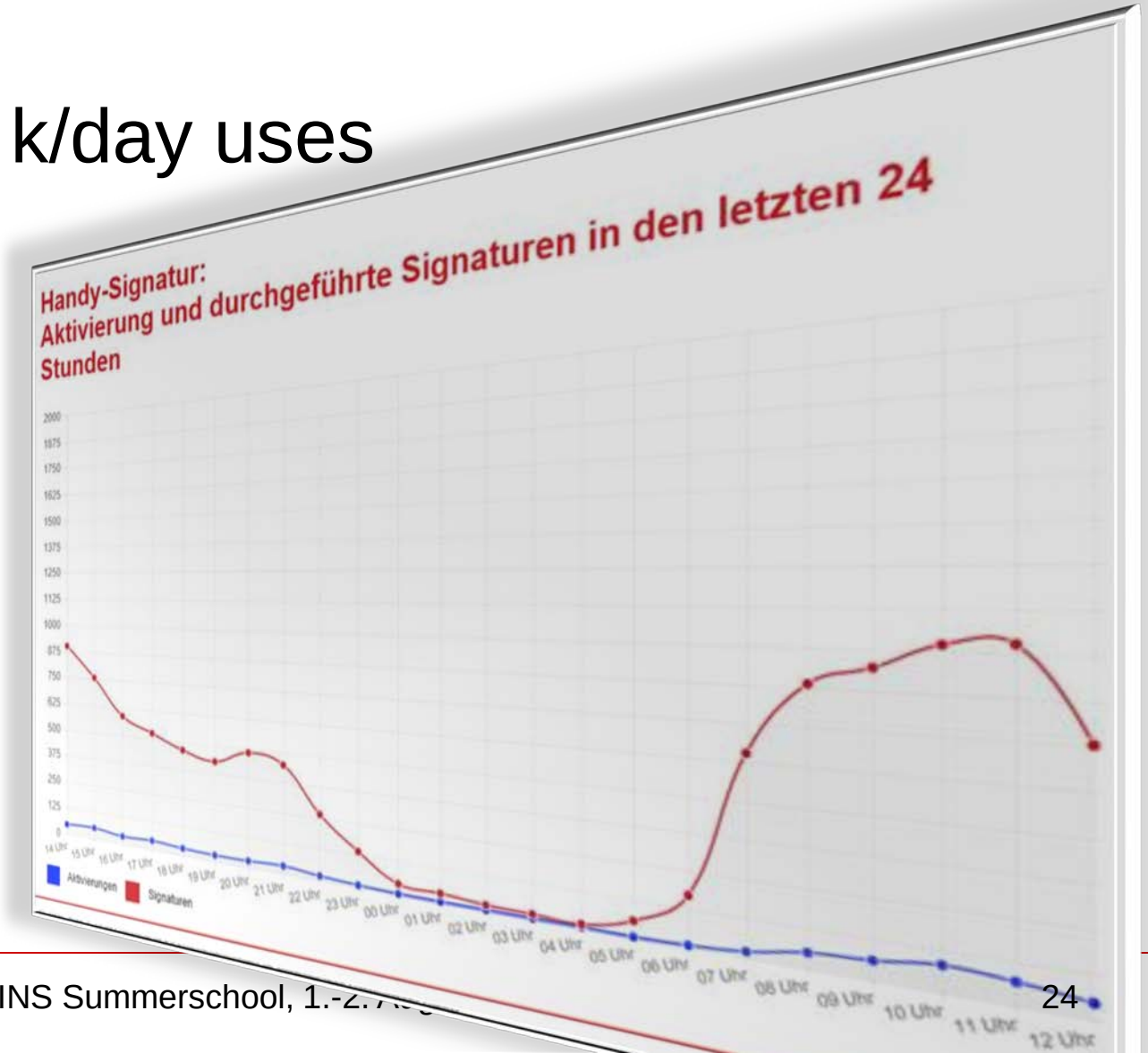
Mobile phone signature
Launched end 2009 through the LSP STORK
Contracted by gvmnt. to a private sector CSP
Success? Well, let's see ...

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

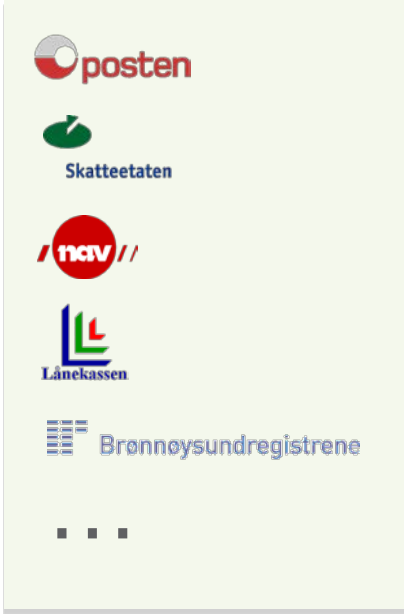
On 21.07.2016 08:18
Digital signatures **301 348 699**
Active cards: **1 272 213**
Electronic authentications: **457 826 295**

- 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

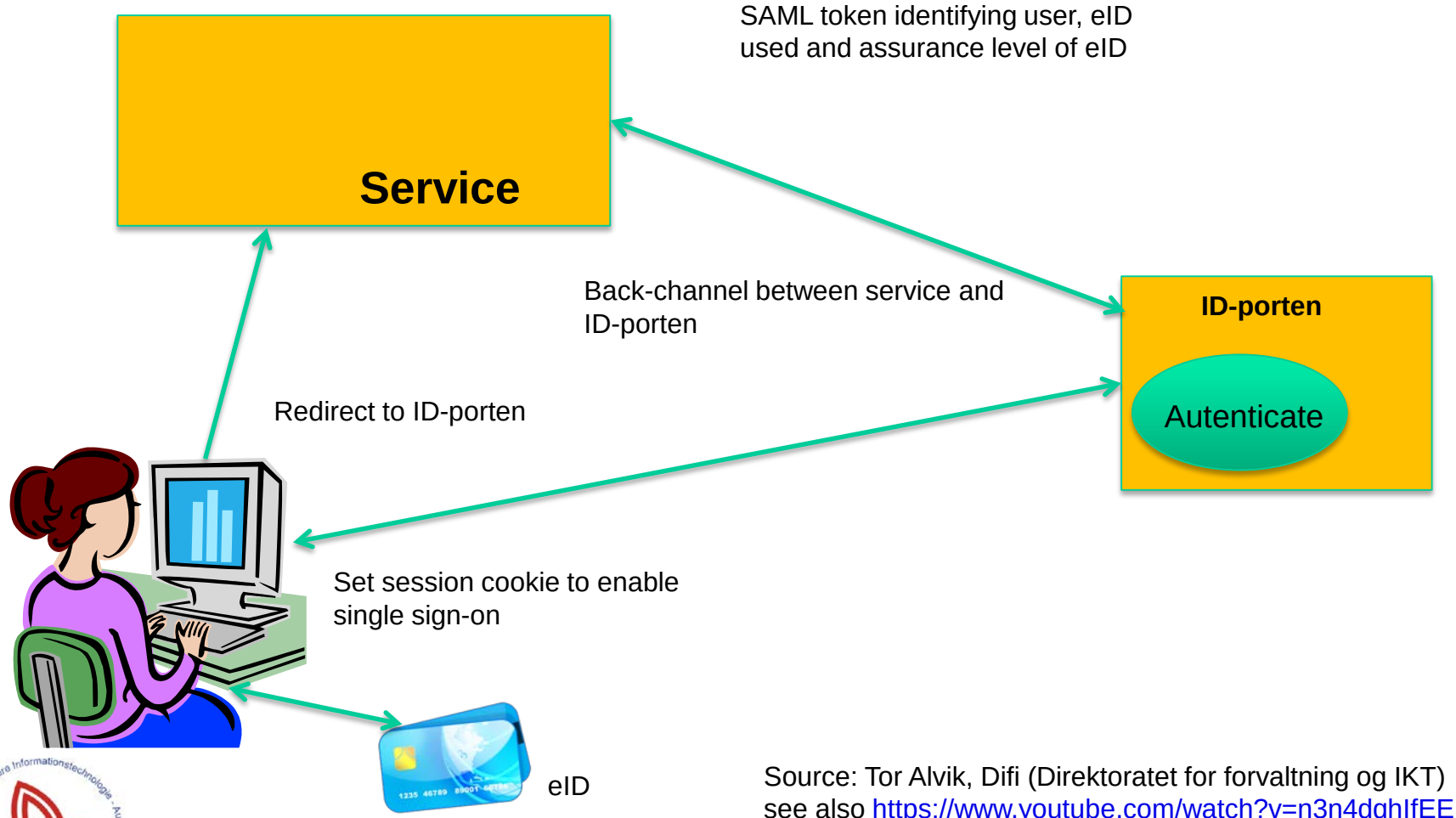
National ID-card with eID is planned for 2018

ID-porten authentication portal.
50 mill transactions in 2014

About 660 services from about 300 (?) public agencies

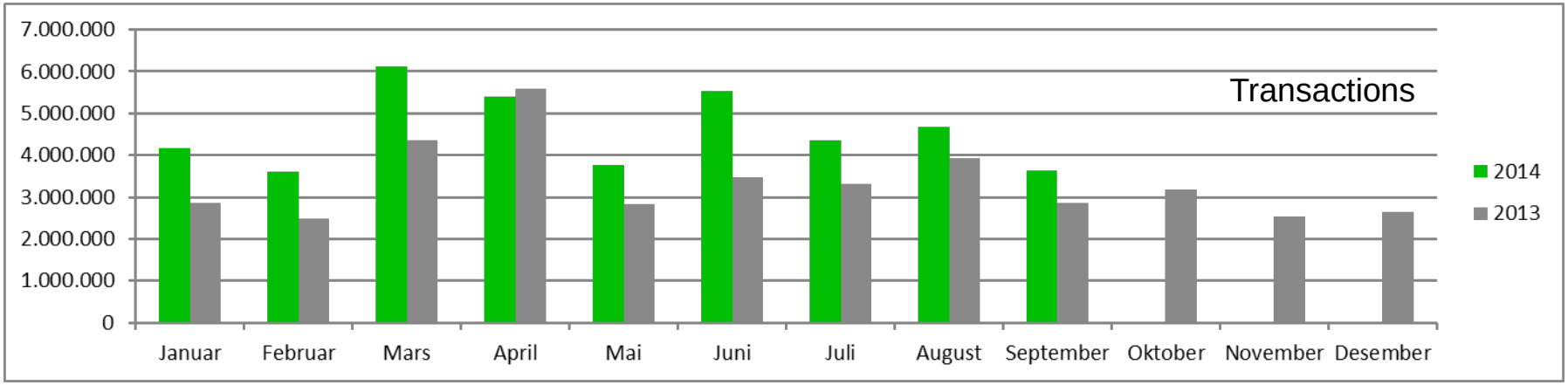
Source: Tor Alvik, Difi (Direktoratet for forvaltning og IKT)
see also https://www.youtube.com/watch?v=n3n4dqhIfEE

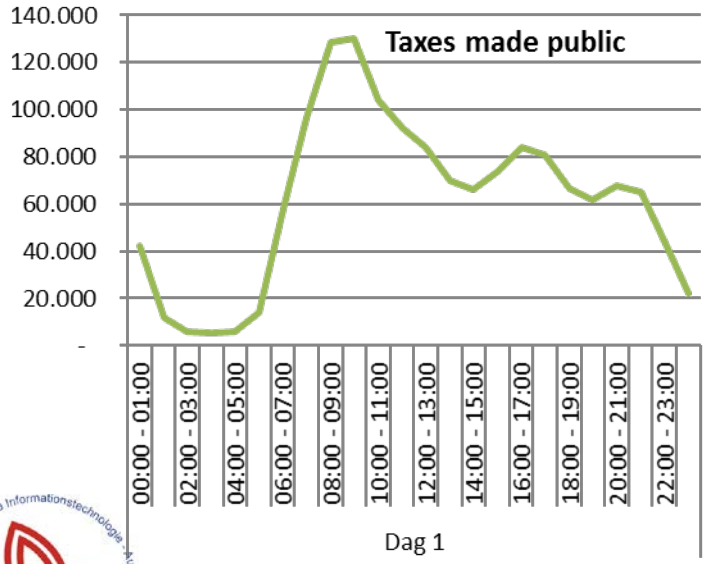
Norway: Authentication process



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

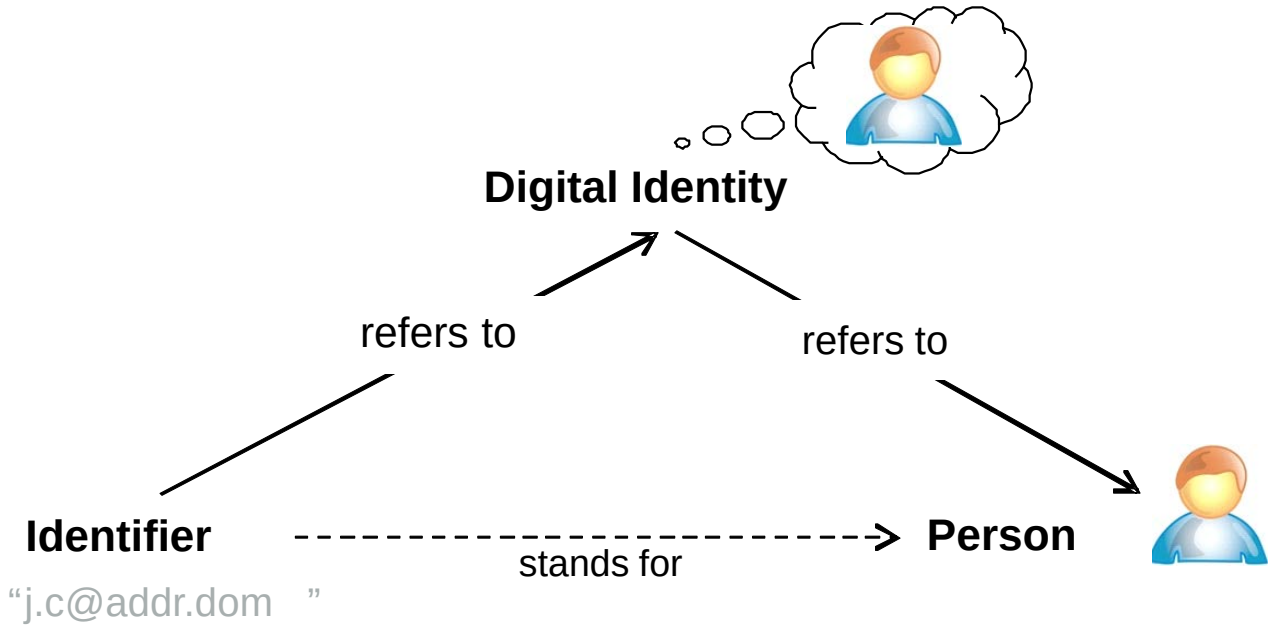
"Digital identity can be defined as the digital representation of the information known about a specific individual or organization. [Bertino and Takahashi]

„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]

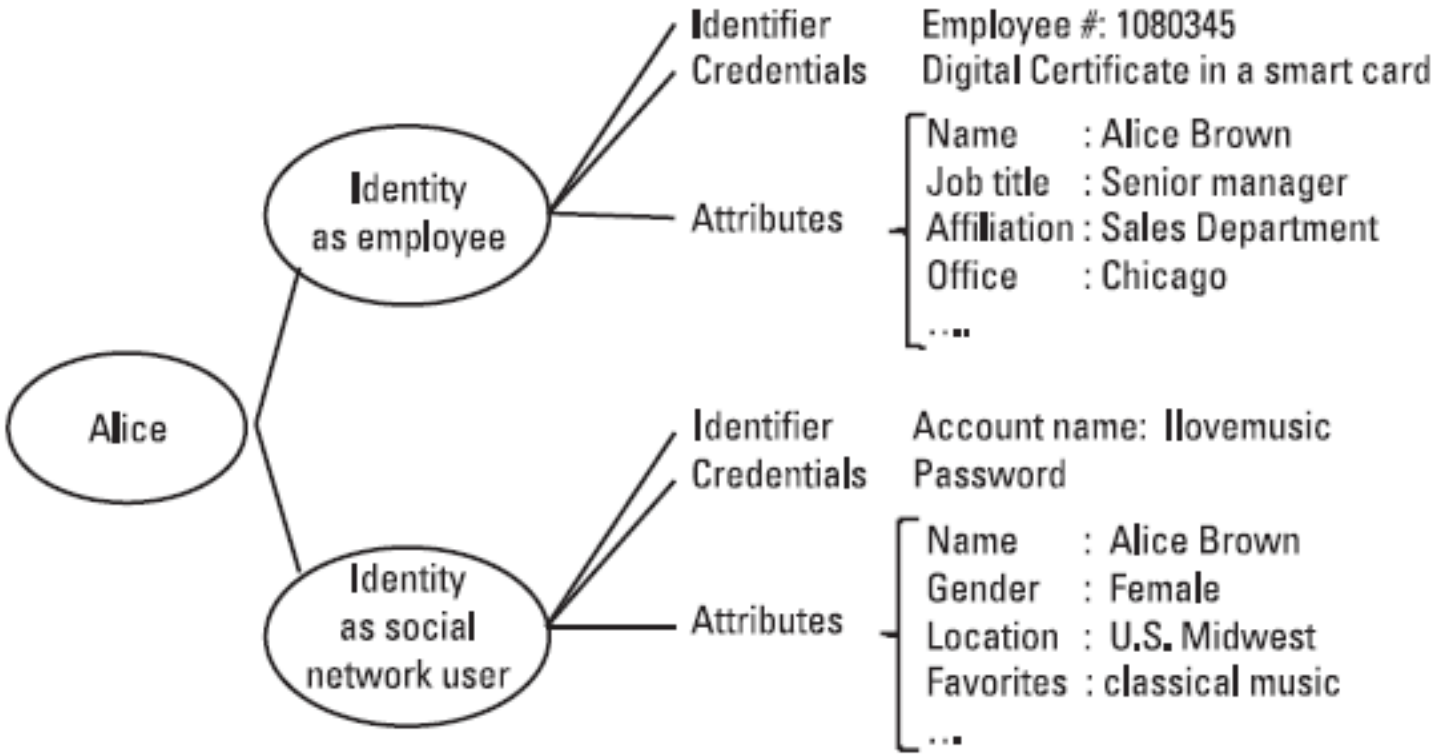
- Same identity properties and attributes, but digitally available
  - E.g.: name, date of birth, …
  - Also: username, e-mail, …
- Applicable also to non-natural persons
  - E.g. a company, …

Digital Identity | Triangle



Ref: GINI-SA

Several Digital Identities



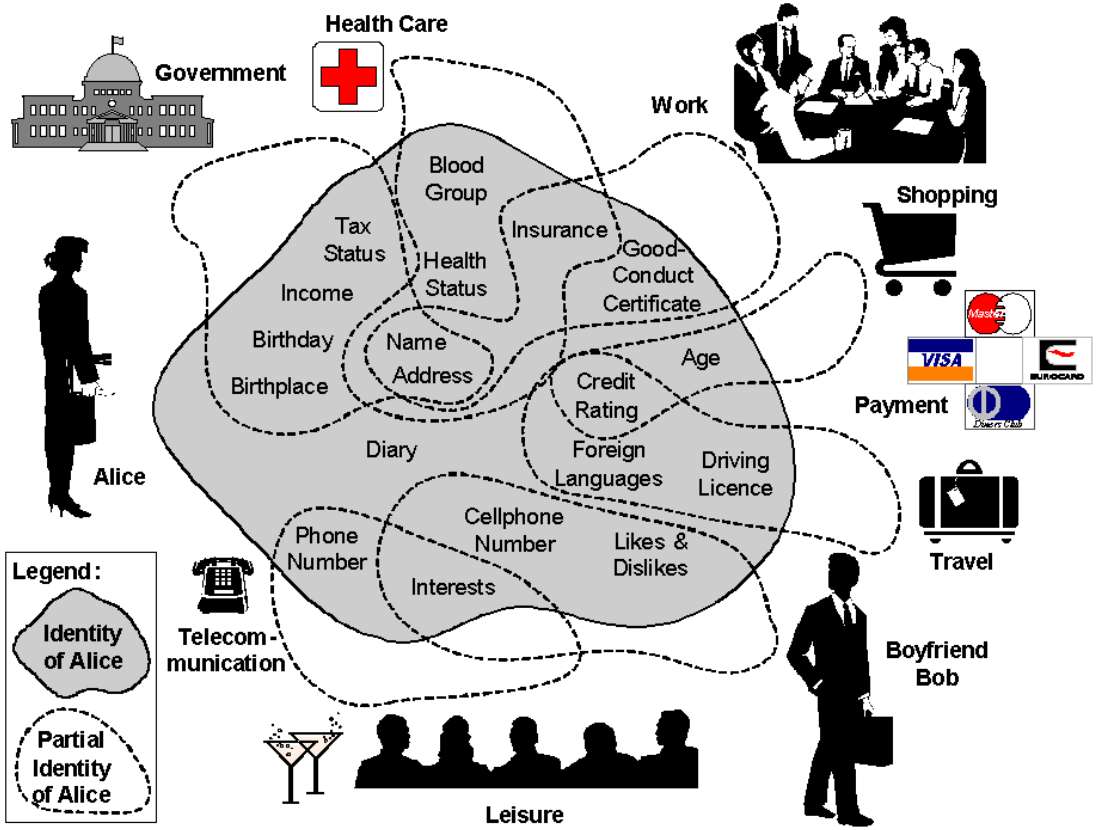
Ref:
Bertino/Takahashi

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

- <u>Pseudonymous identities</u>
  - 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
- <u>Anonymous identities</u>
  - Decouple the digital identity from the real person
  - Unlinkability to real person
  - Normally temporary and for single transactions
  - E.g. completing a questionnaire

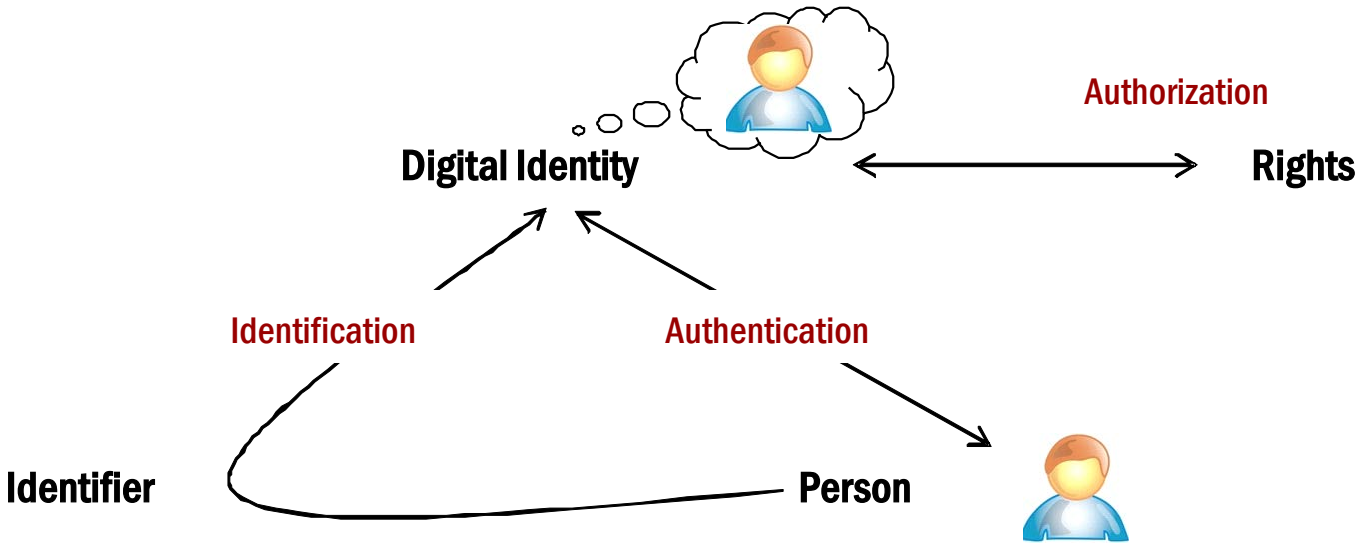
Identity Types

- 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

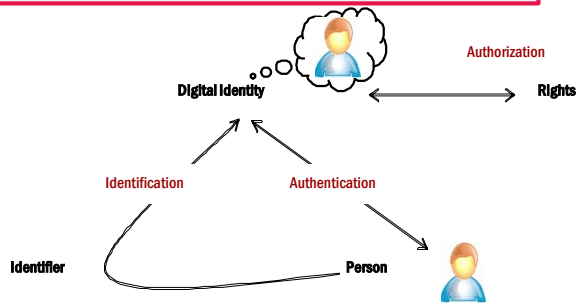


Ref: GINI-SA

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

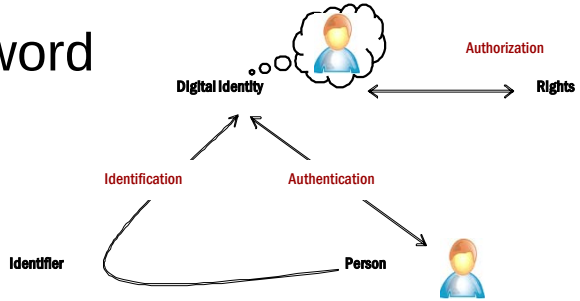
Authentication is proof of an attribute. [Clarke]

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

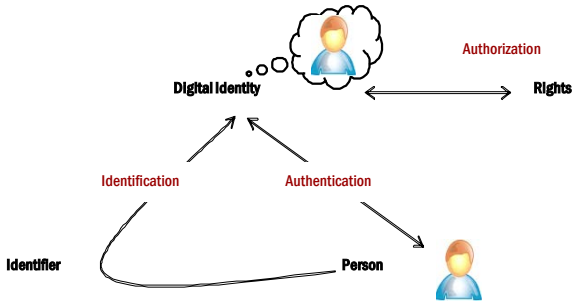
- Combining different authentication mechanisms to increase security
- E.g. Ownership and Knowledge (2-factor)
  - Citizen card (smart card and PIN)
  - Mobile phone signature (mobile phone and password)
- Increased security by increasing the number of mechanisms

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

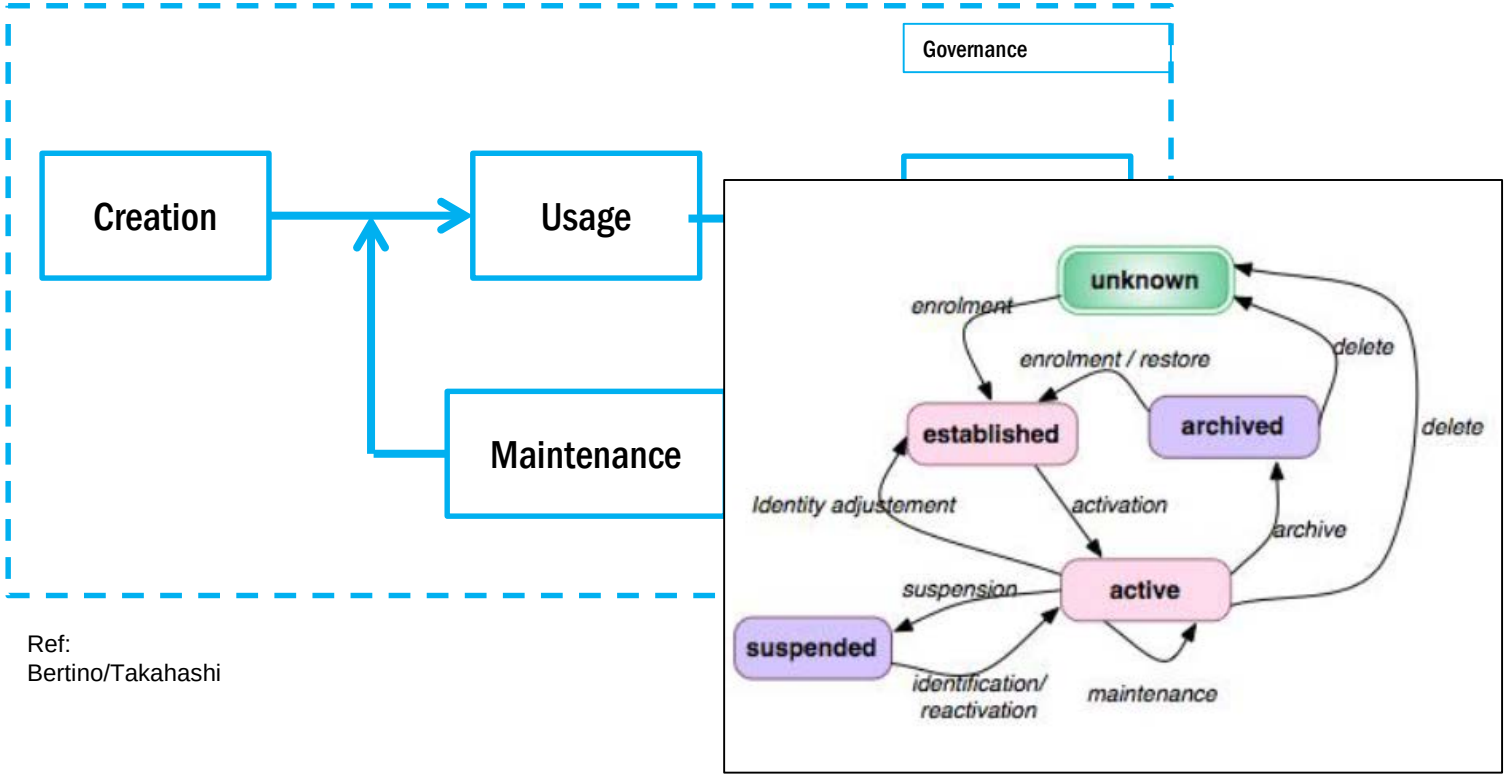
- Identity
  - “Jane Doe“
- Identification
  - “I am Jane Doe“
- Authentication
  - “My passport proves that I am Jane Doe”
- Authorization
  - “Jane Doe is employed at company A and is allowed to access service B”

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, …

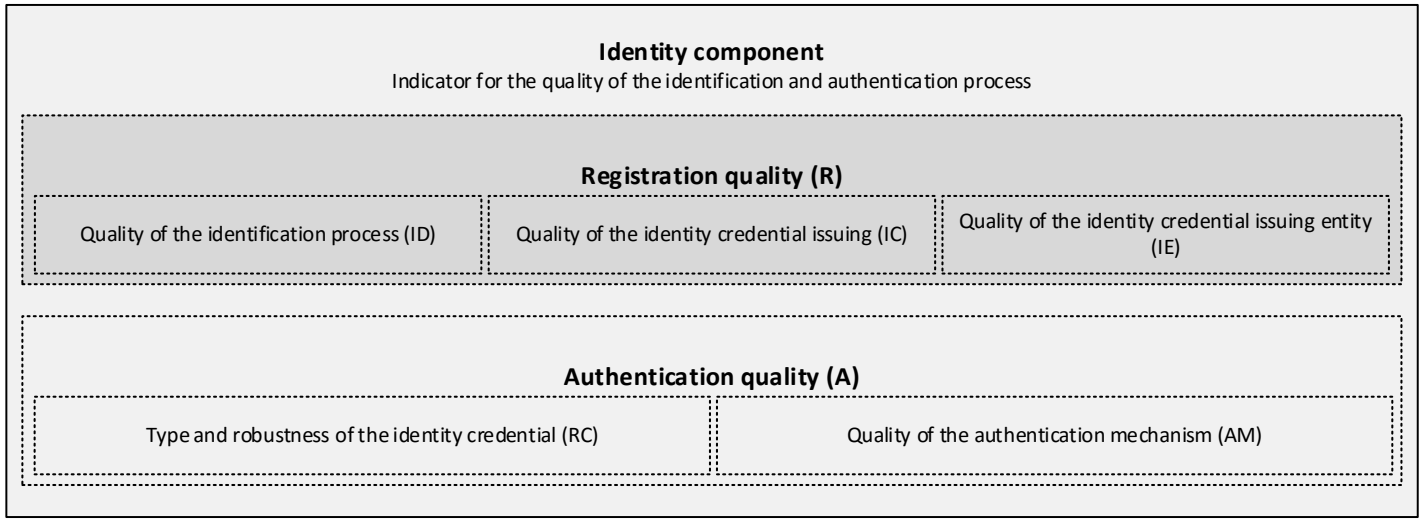
ISO/IEC 29115

	Technical		Management & Organizational
Enrolment phase	• Application and initiation • Identity proofing and identity information verification	• Record-keeping/ recording • Registration	• Service establishment • Legal and contractual compliance • Financial provisions • Information security management and audit • External service components • Operational infrastructure • Measuring operational capabilities
Credential management phase	• Credential creation •Credential pre-processing • Credential issuance • Credential activation • Credential storage	• Credential suspension, revocation, and/or destruction • Credential renewal and/or replacement • Record-keeping	
Entity authentication phase	• Authentication • Record-keeping		

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

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

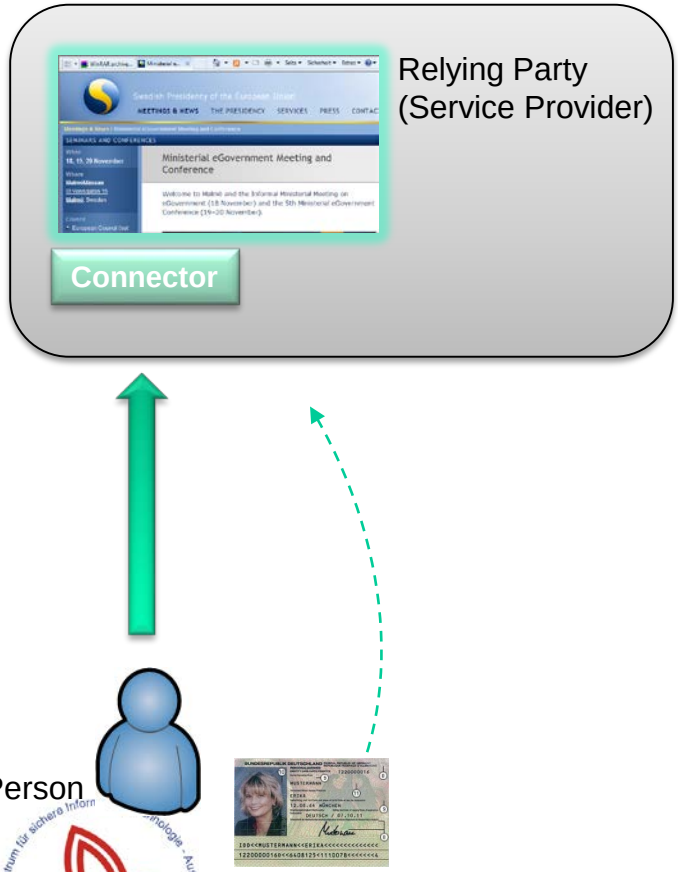
"The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies."

Contents

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

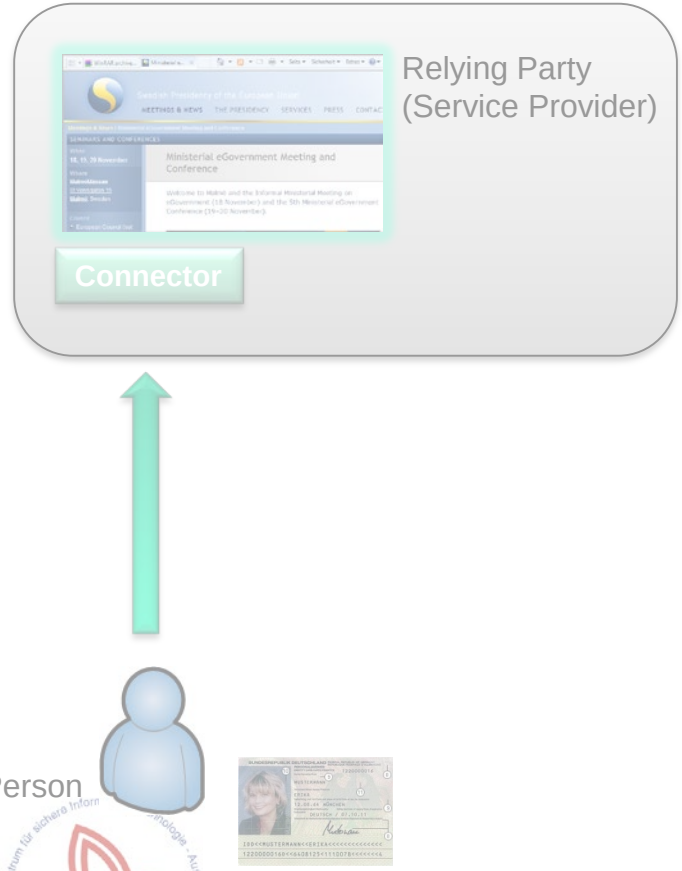
Direct vs. Indirect authentication

Direct Authentication

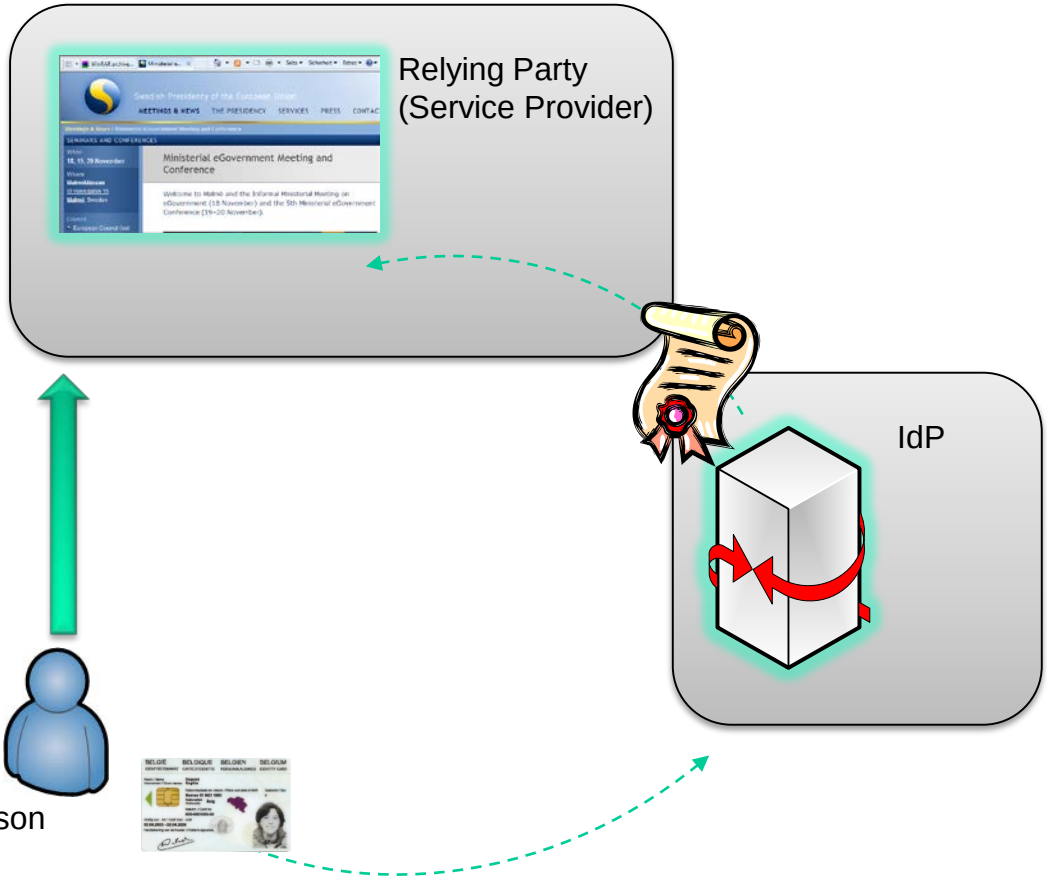


Direct vs. Indirect authentication

Direct Authentication



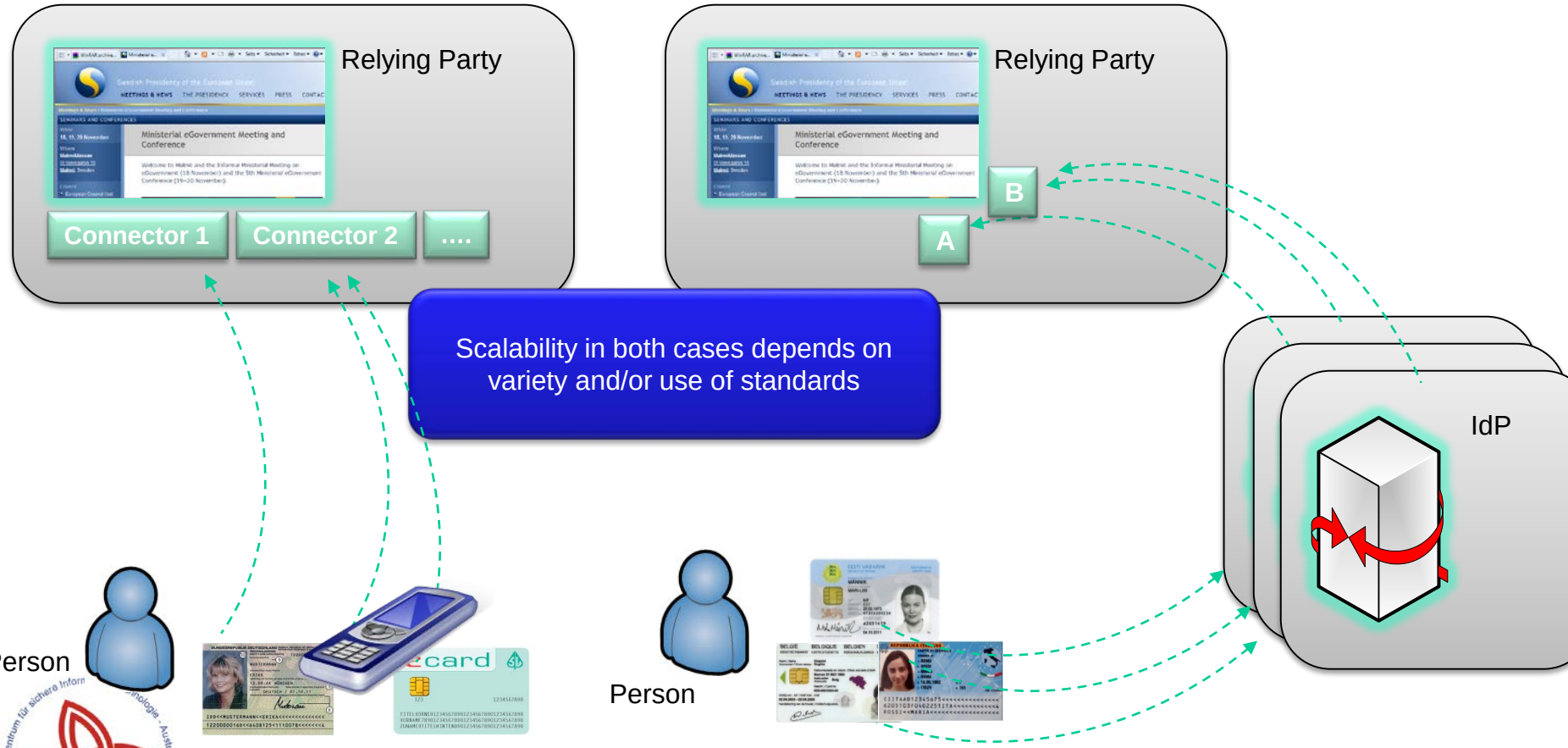
Indirect (IdP-based) Authentication

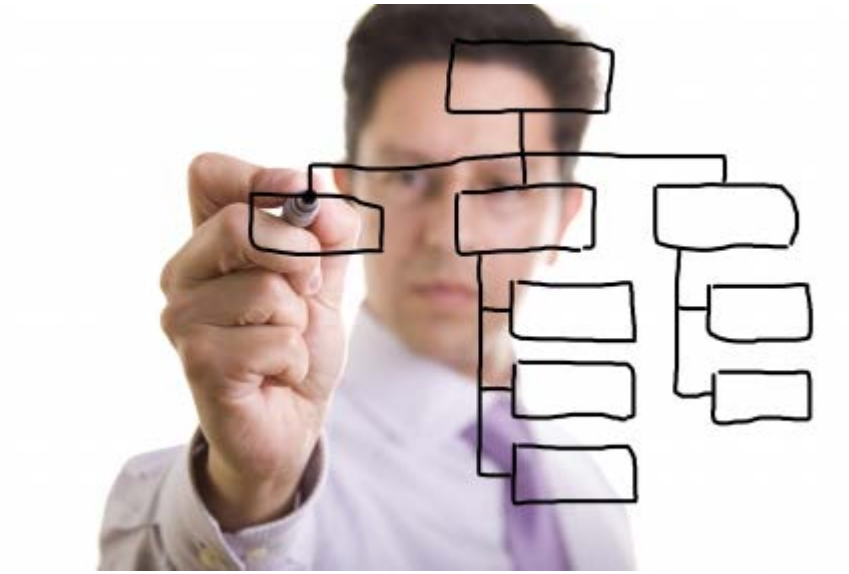


What if there are several eID schemes?

Direct Authentication

Indirect (IdP-based) Authentication

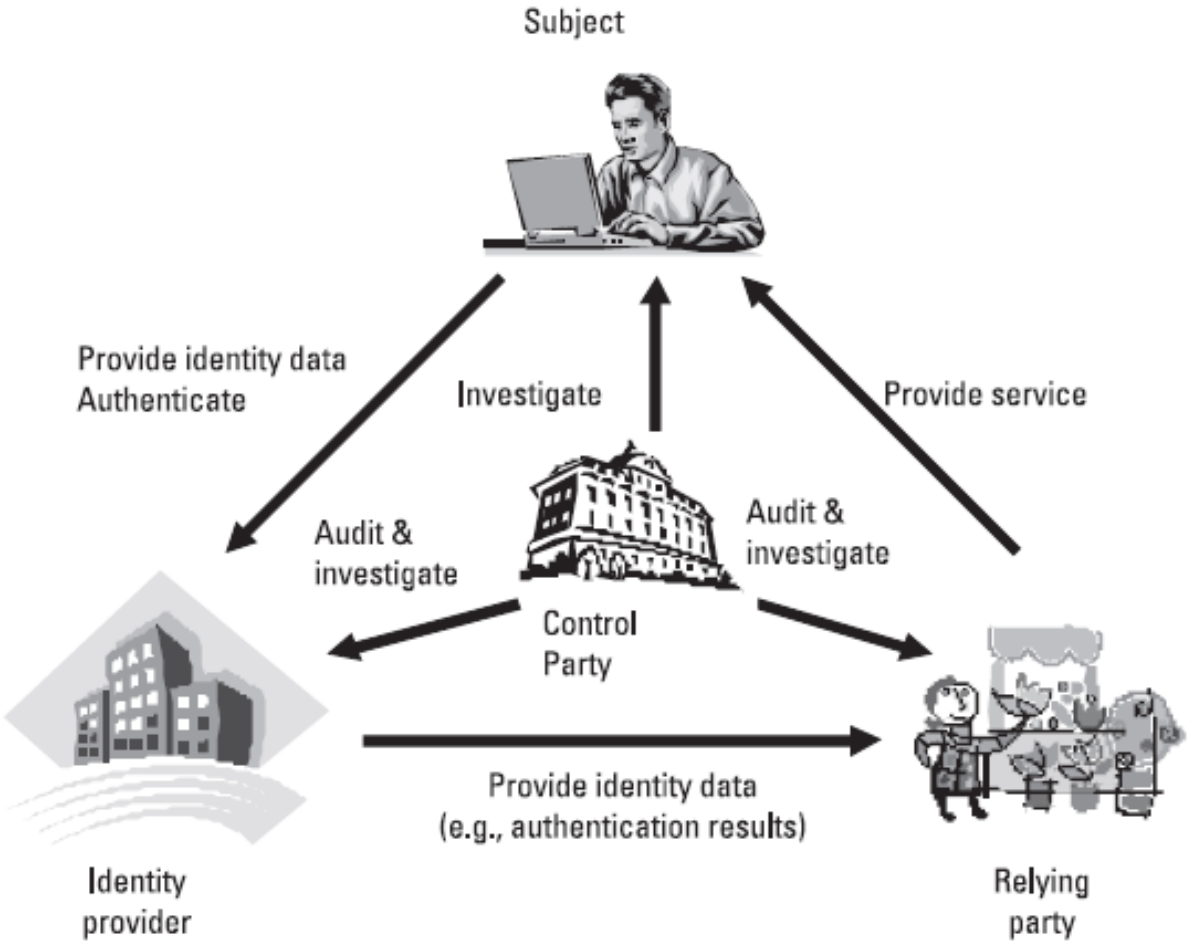




SECTION 5: ARCHITECTURES

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

Stakeholders

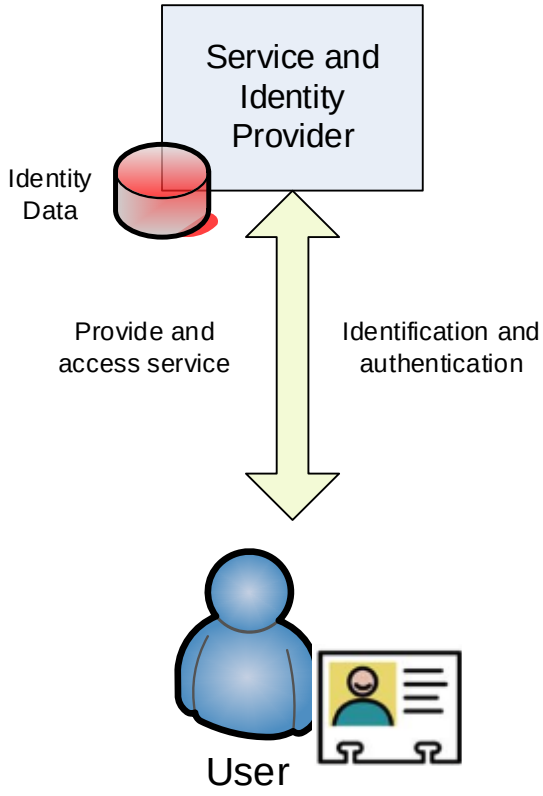


Ref:
Bertino/Takahashi

Stakeholders

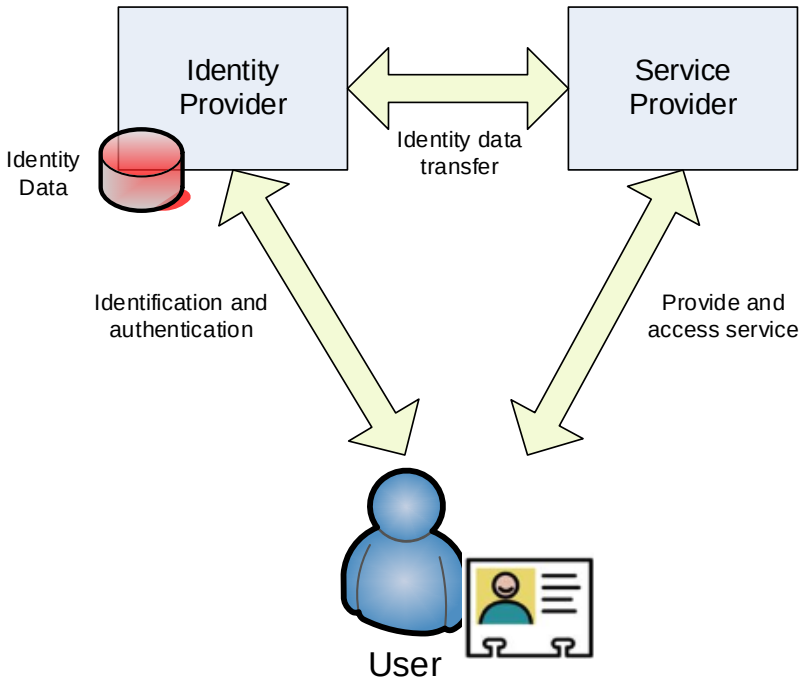
- Subject
  - Digital identity of a person
  - Provides identity data (attributes) to the identity provider
- Identity Provider (IdP)
  - Provides identity data of the subject to the service provider
  - Identification, Authentication (and Authorization)
- Relying Party (Service Provider - SP)
  - Provides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



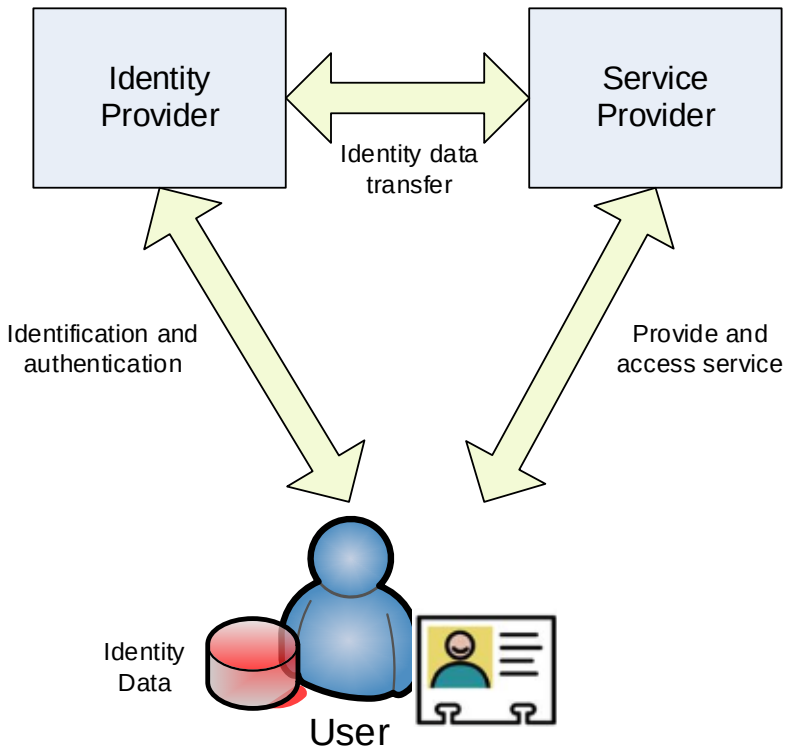
- Service Provider and Identity Provider merge
- Authentication directly at the Service Provider
- IdM system only applicable for specific Service Provider
- Identity data stored and maintained at the individual Service Provider

Central Model



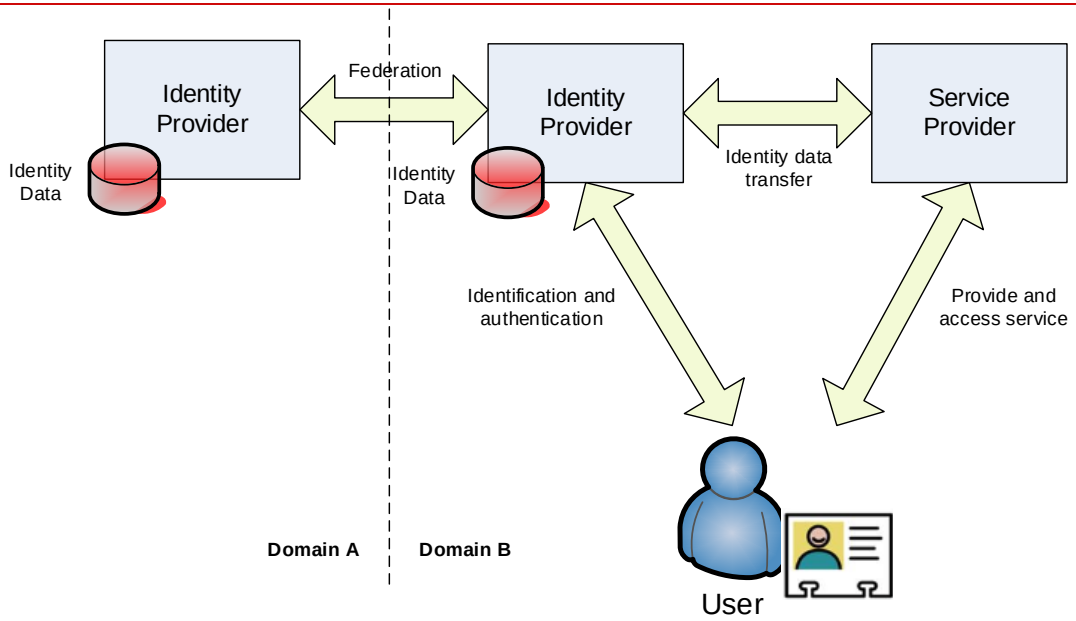
- Identity Provider (IdP) stores identity data
- IdP provides identity data to the service provider (SP)
- User has no control on actual data transfer
- e.g., Central Authentication Service (CAS), Facebook

User-Centric Model



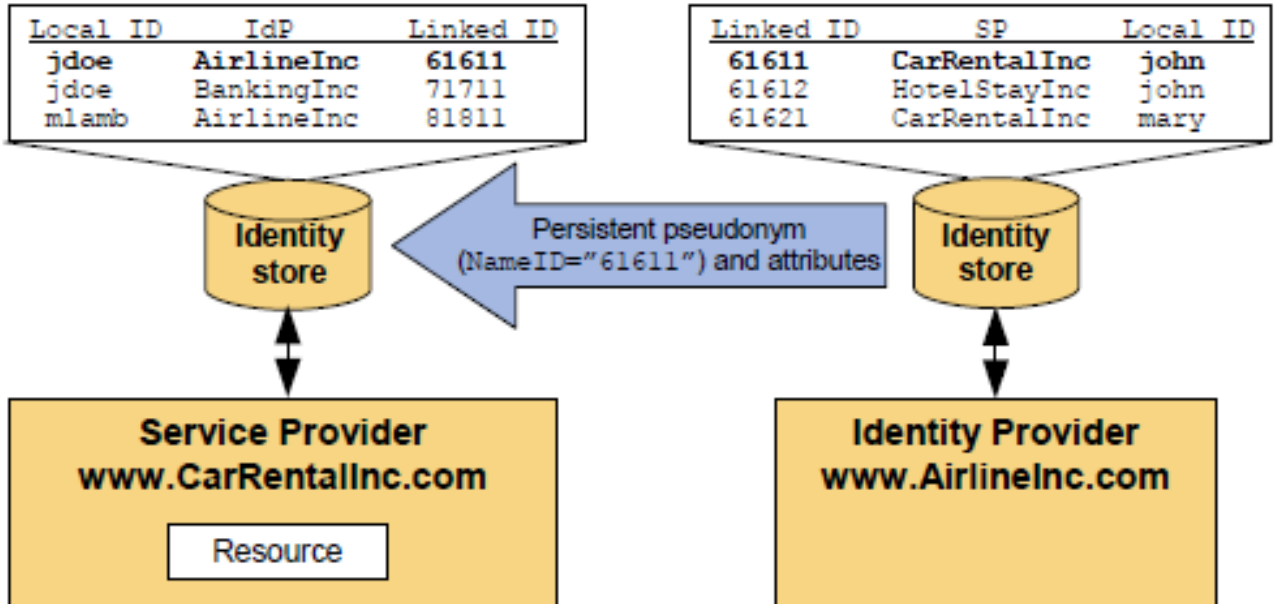
- Identity data stored in user-domain
- Usually stored on a secure token (e.g., smart card)
- Explicit user consent
- e.g., Austrian Citizen Card, German nPA

Federated Model



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

Identity Federation

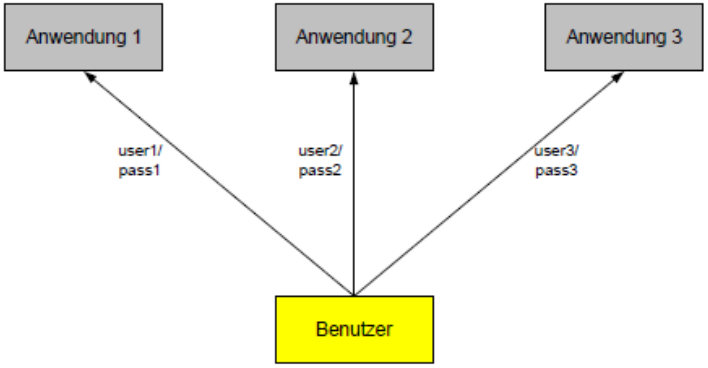


Ref: SAML 2.0 Technical Overview

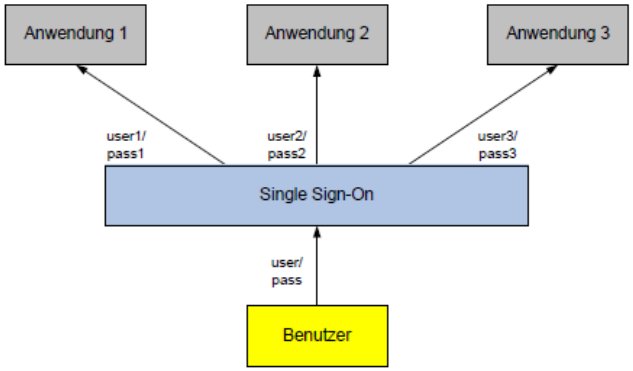
Single Sign-On (SSO)

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

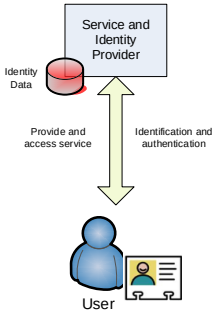
Single Logout (SLO)

- 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

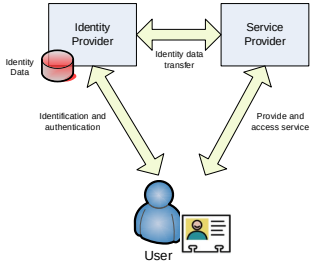
Trust Management

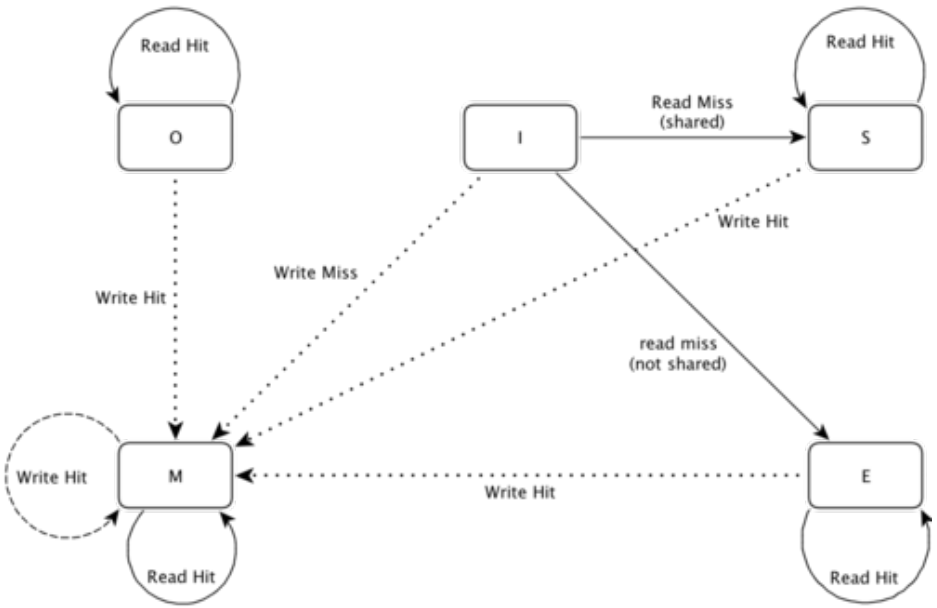
"Trust is the characteristic whereby one entity is willing to rely upon a second entity to execute a set of actions and/or to make a set of assertions about a set of principals and/or digital identities. In the general sense, trust derives from some relationship (typically a business or organizational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

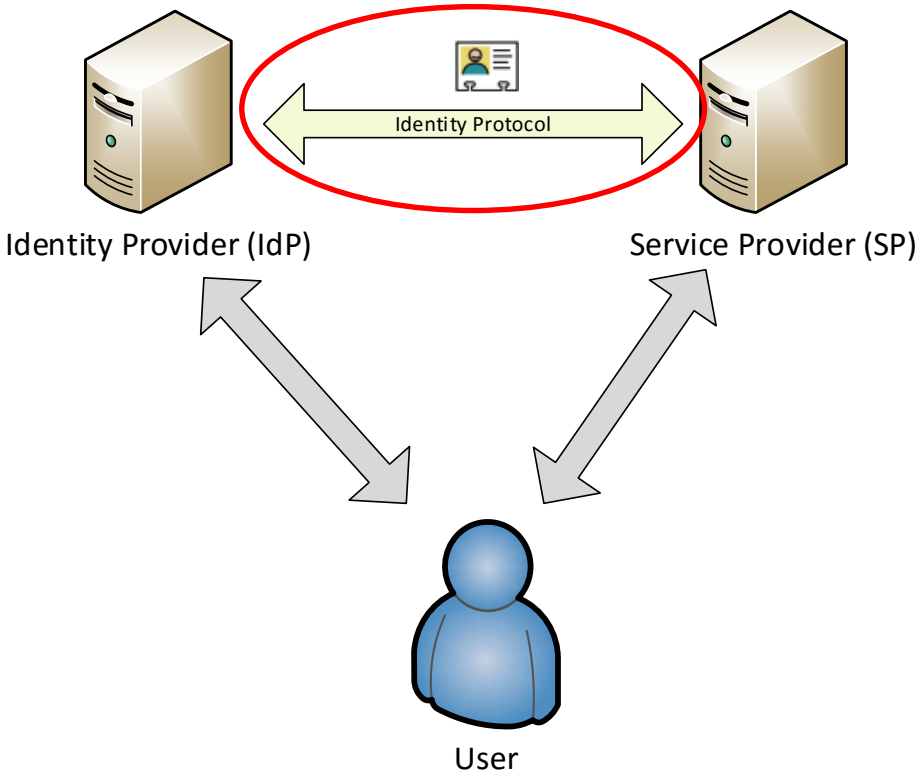




SECTION 6: PROTOCOLS

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

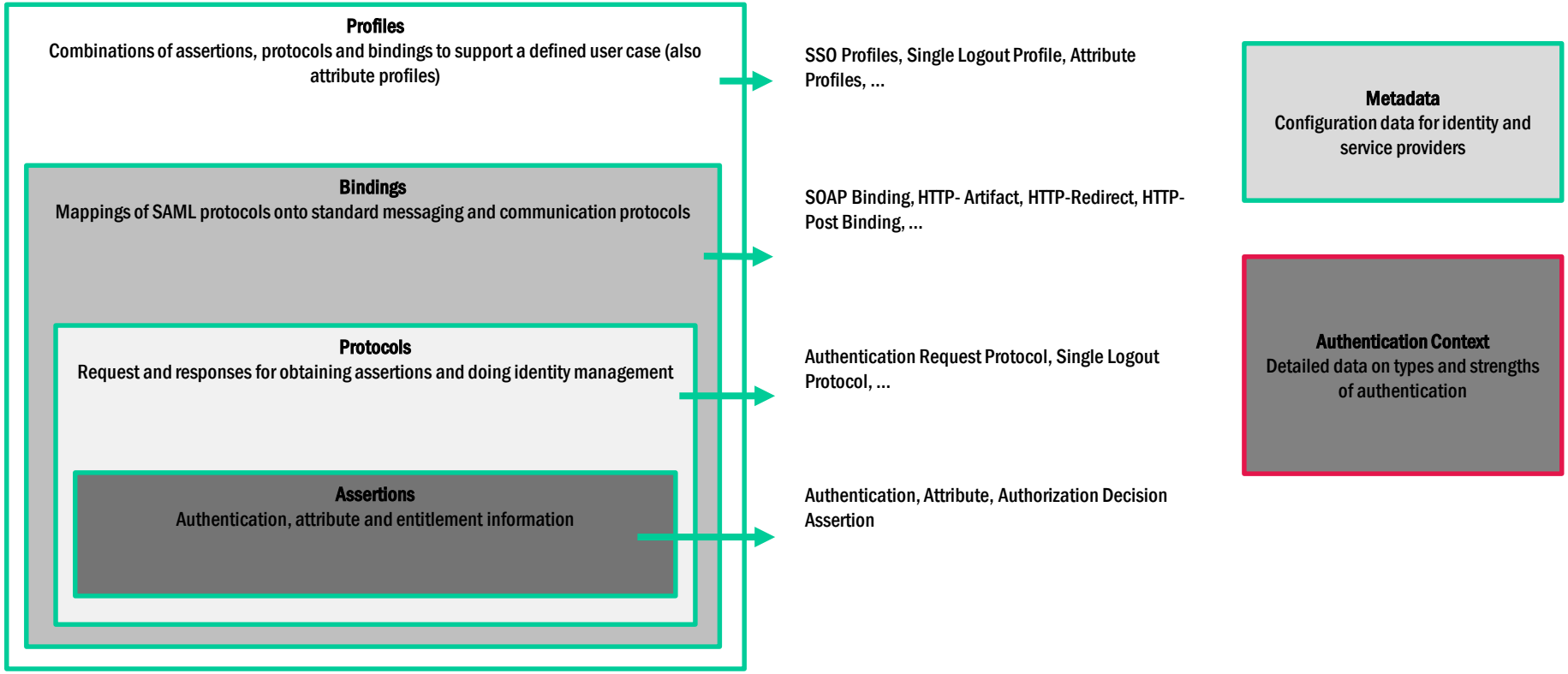
SAML | Security Assertion Markup Language

- 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

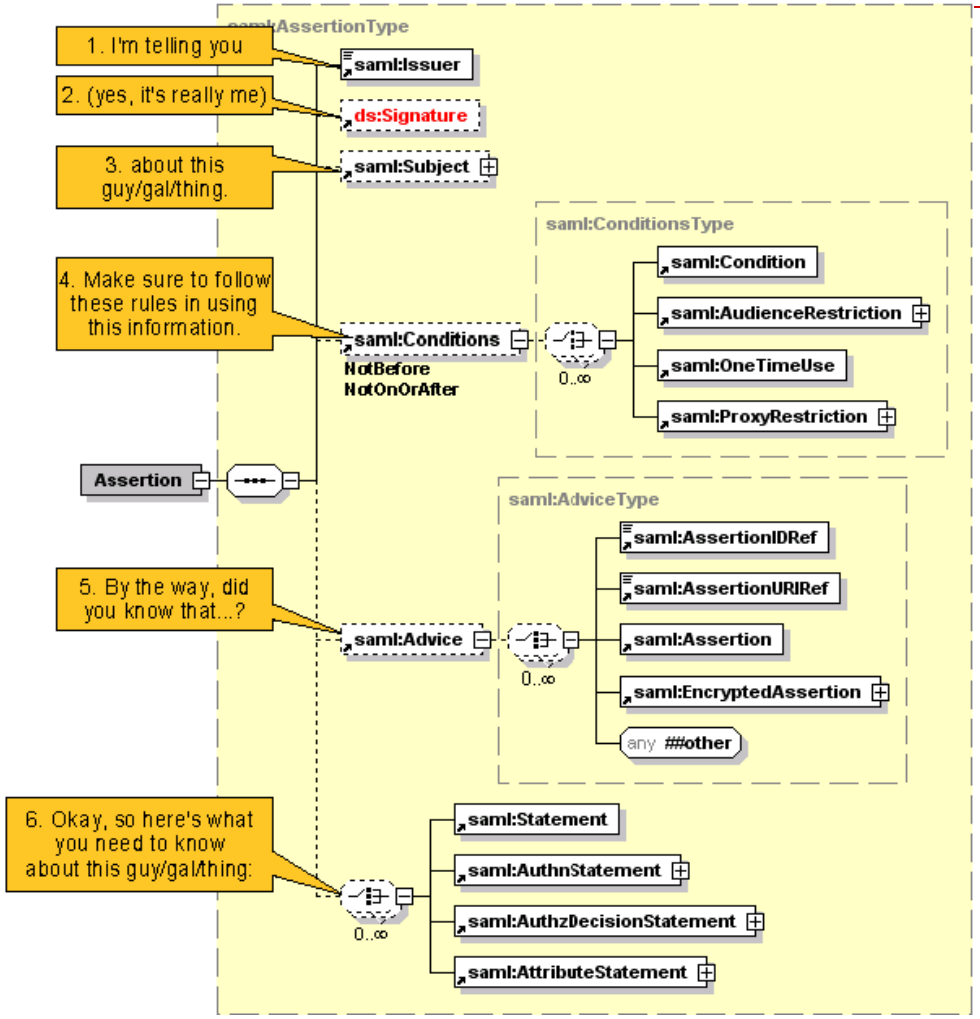


Ref: SAML 2.0 Technical Overview

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

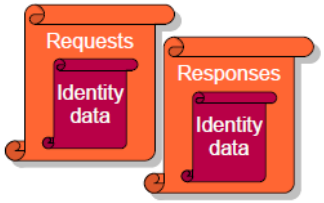
SAML Authentication Statement

SAML Attribute Statement

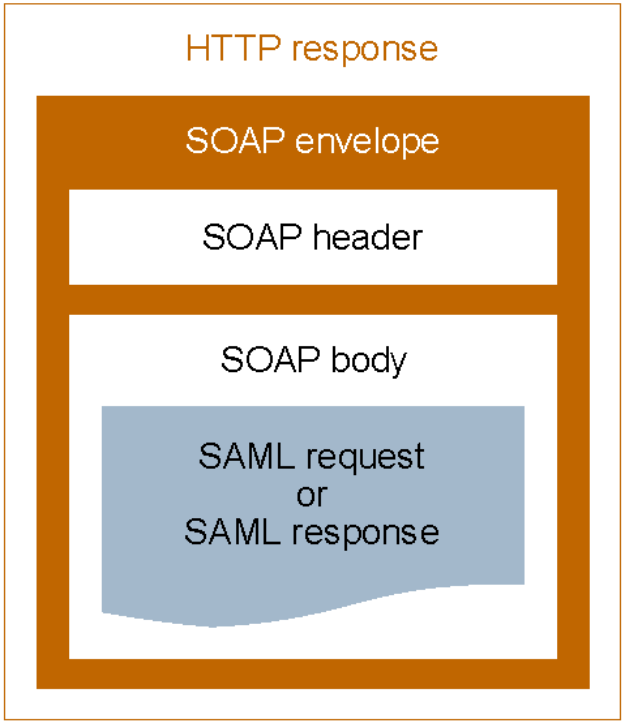
Ref: Eve Maler

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)



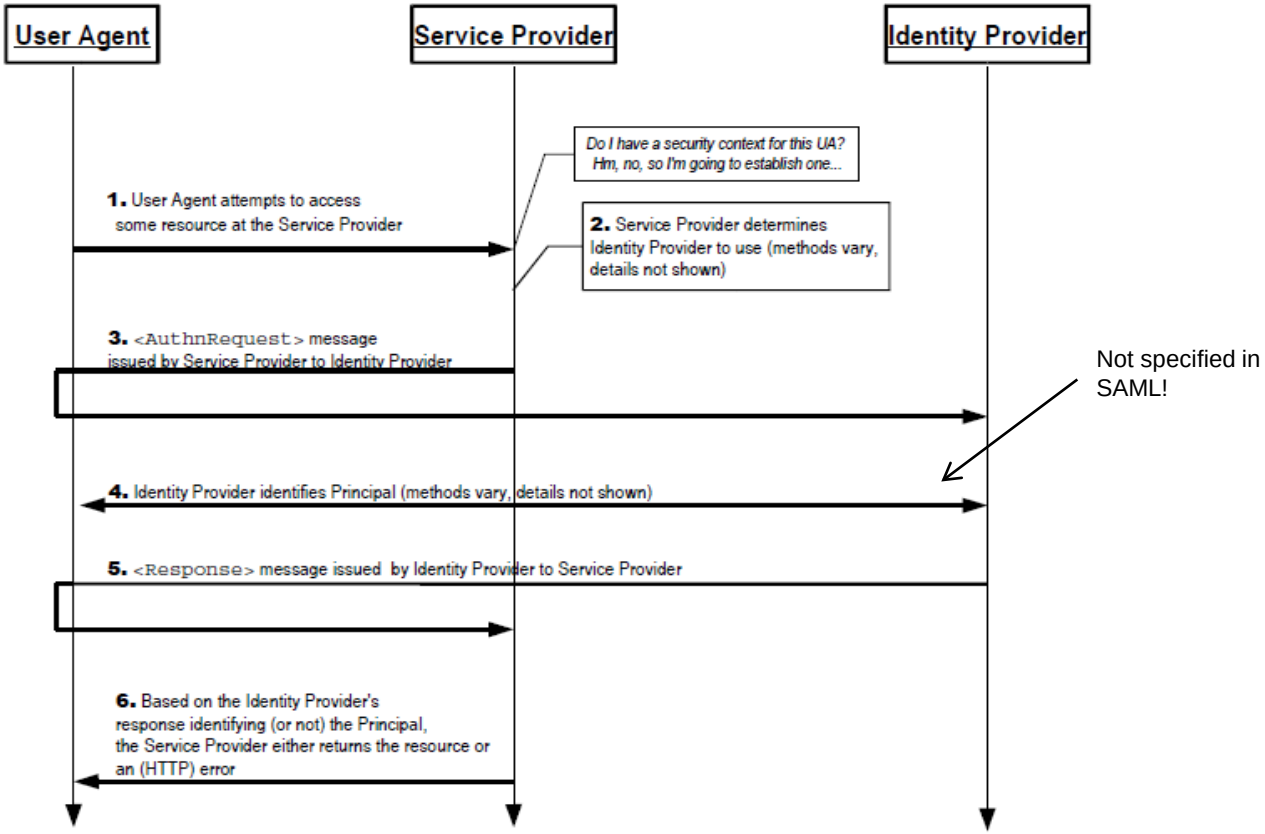
protocol-SOAP-HTTP

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope
  xmlns:env="http://www.w3.org/2003/05/soap/envelope/">
  <env:Body>
    <samlp:AttributeQuery
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
      ID="aaf23196-1773-2113-474a-fe114412ab72"
      Version="2.0"
      IssueInstant="2006-07-17T20:31:40Z">
      <saml:Issuer>http://example.sp.com</saml:Issuer>
      <saml:Subject>
          <saml:NameID
          Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
          C=US, O=NCSA-TEST, OU=User, CN=trscavo@uiuc.edu
          </saml:NameID>
      </saml:Subject>
      <saml:Attribute
          NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
          Name="urn:oid:2.5.4.42"
          FriendlyName="givenName">
      </saml:Attribute>
     </samlp:AttributeQuery>
  </env:Body>
</env:Envelope>
```

SAML | Profiles

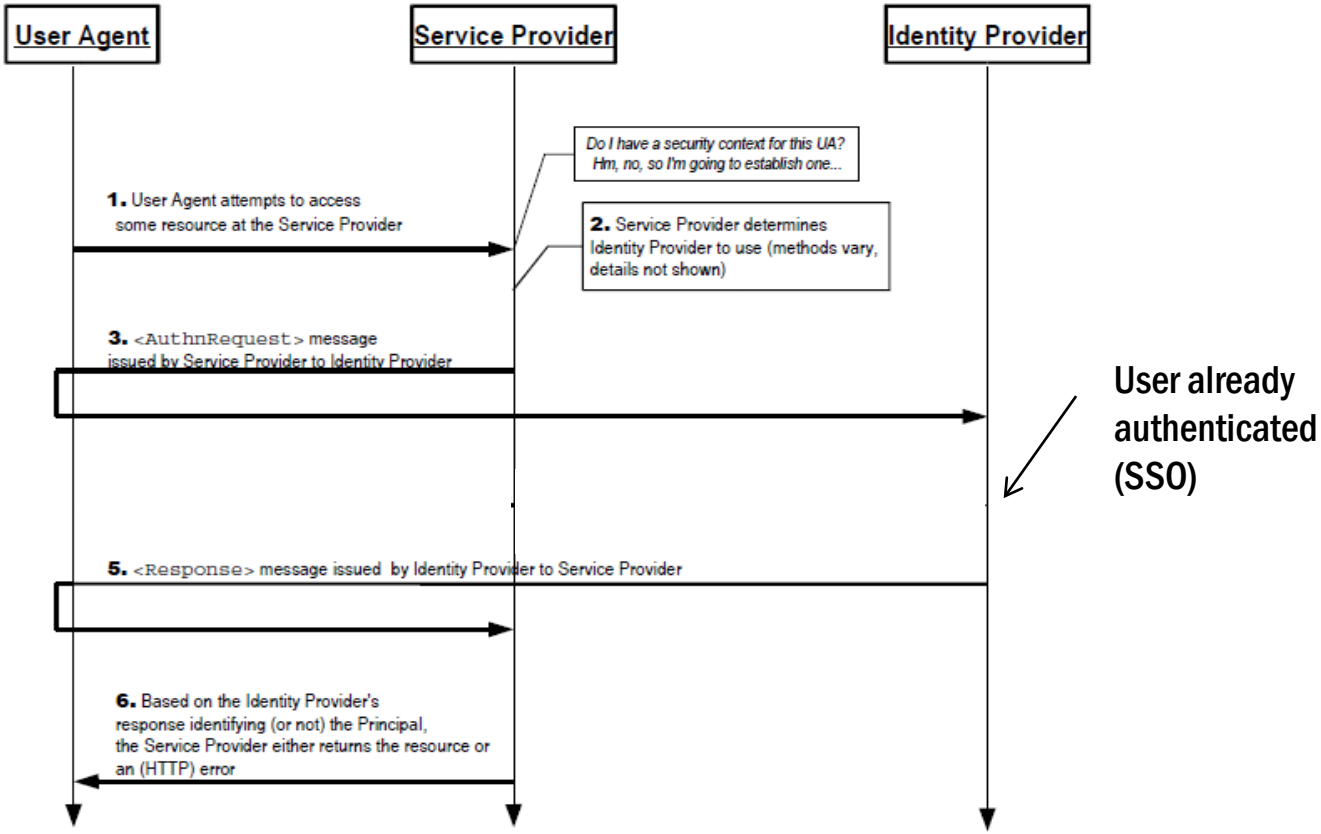
- Model the SAML use cases by combining SAML Assertions, SAML Protocols and SAML Bindings
  - Single sign-on, identity federation, single logout, …
- Profiles are standardized but own profiles may be created
  - E.g. Kantara, STORK, eIDAS specification, …

SAML | Login Process



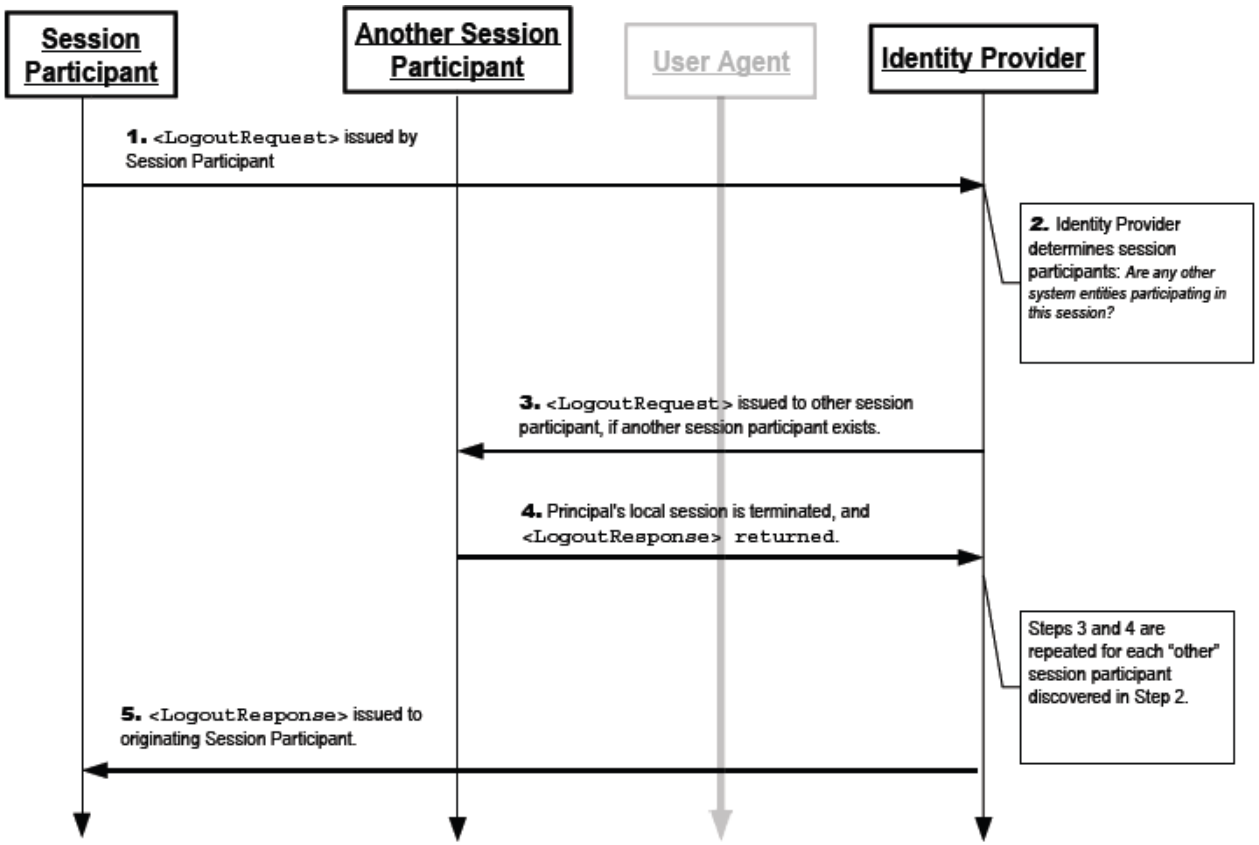
Ref: SAML 2.0 Core

SAML | SSO Login Process



Ref: SAML 2.0 Core

SAML | Single Logout Process



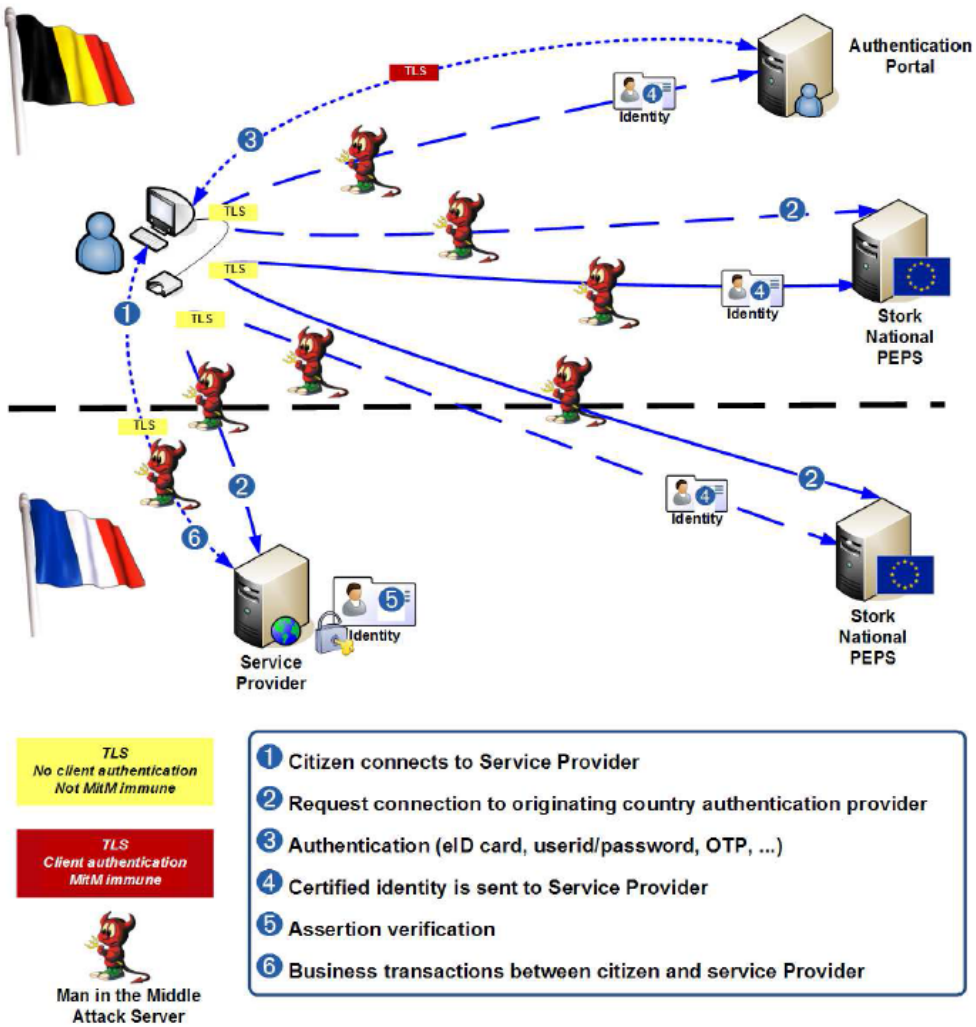
Ref: SAML 2.0 Core

SAML Holder-of-key (HoK) Profile

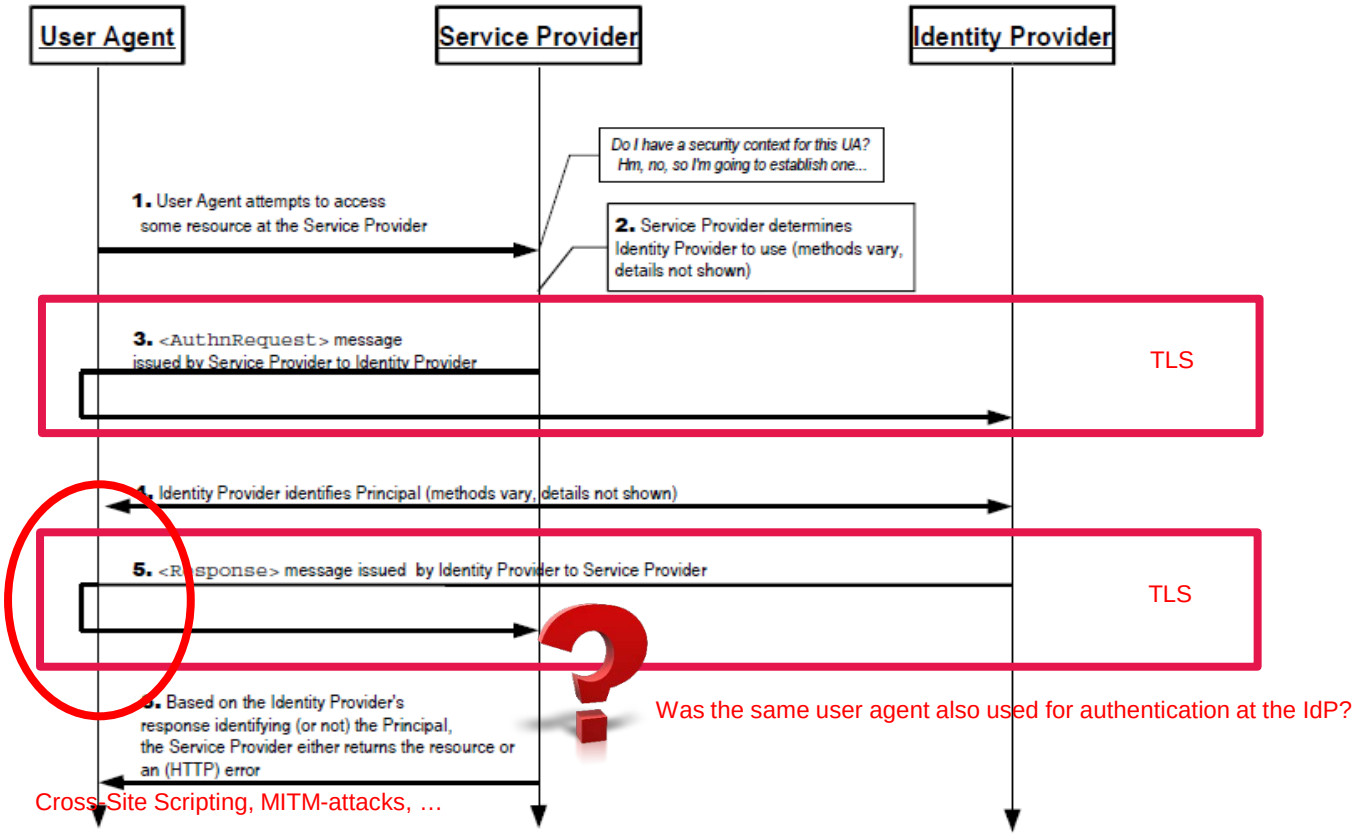
- Enhance the security of SAML message exchange without requiring modifications to client software
- Stronger security context between IdP and SP
- Use of underlying TLS session and X.509 certificates
- Cryptographic binding between SAML assertion and user agent due to the use of TLS client certificates (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 …

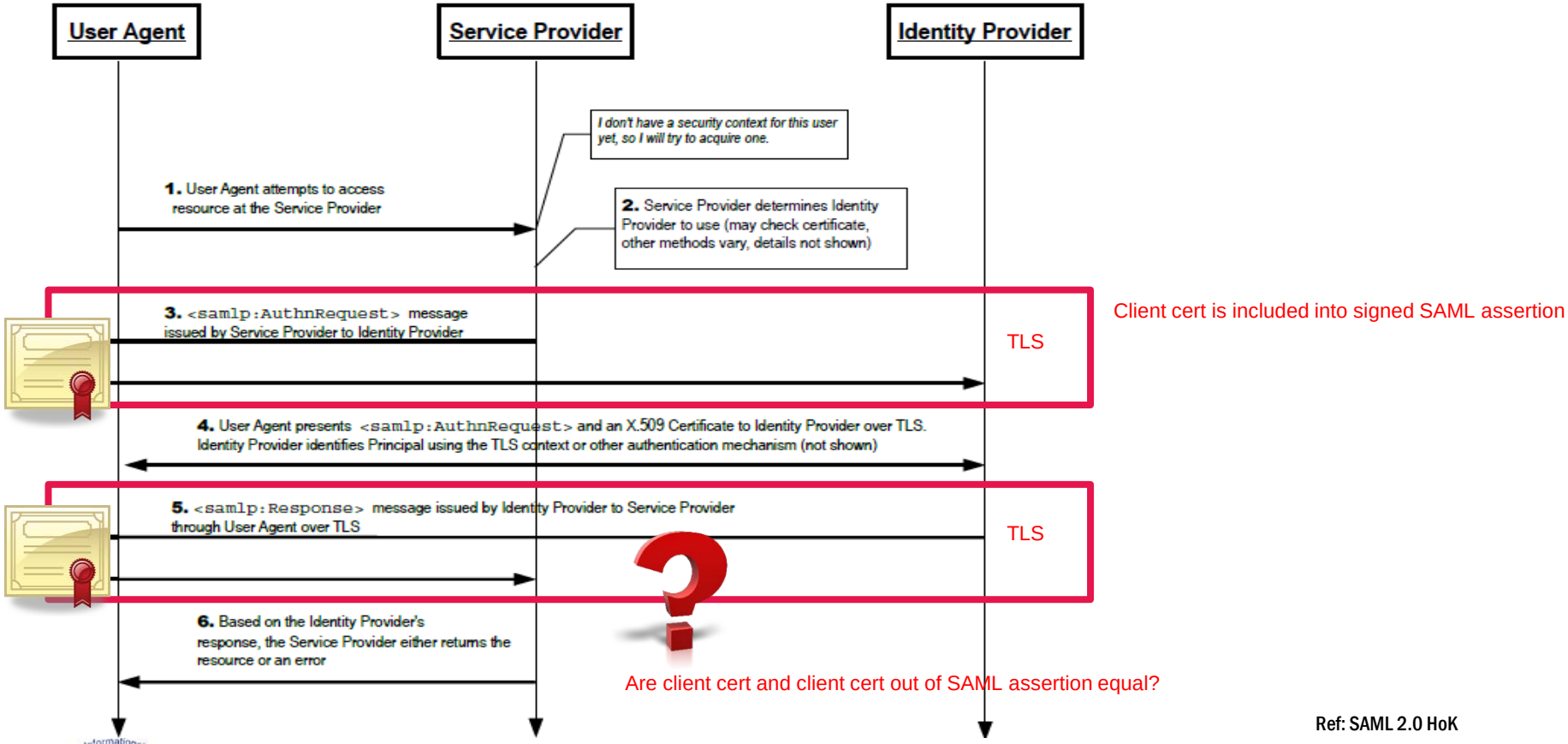


SAML | Standard Login Process



Ref: SAML 2.0 Core

SAML | HoK Login Process



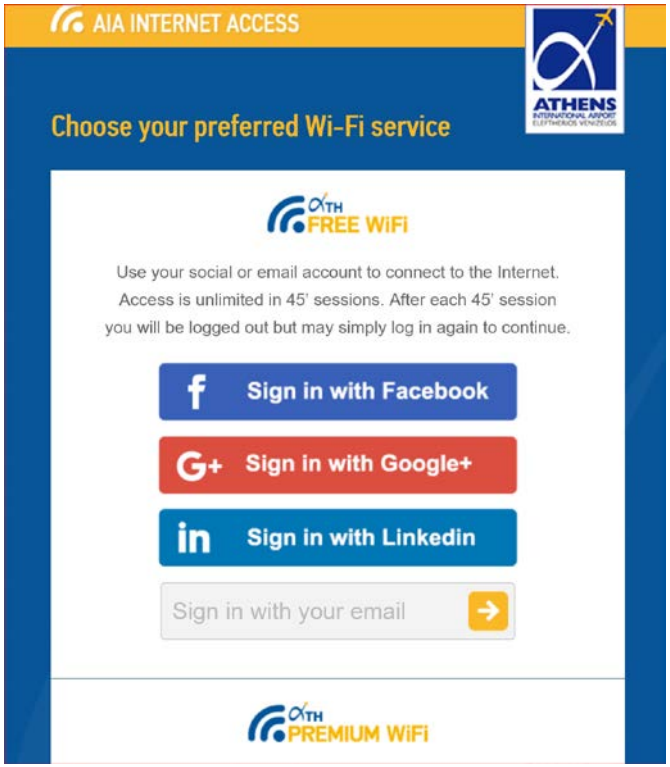
Ref: SAML 2.0 HoK

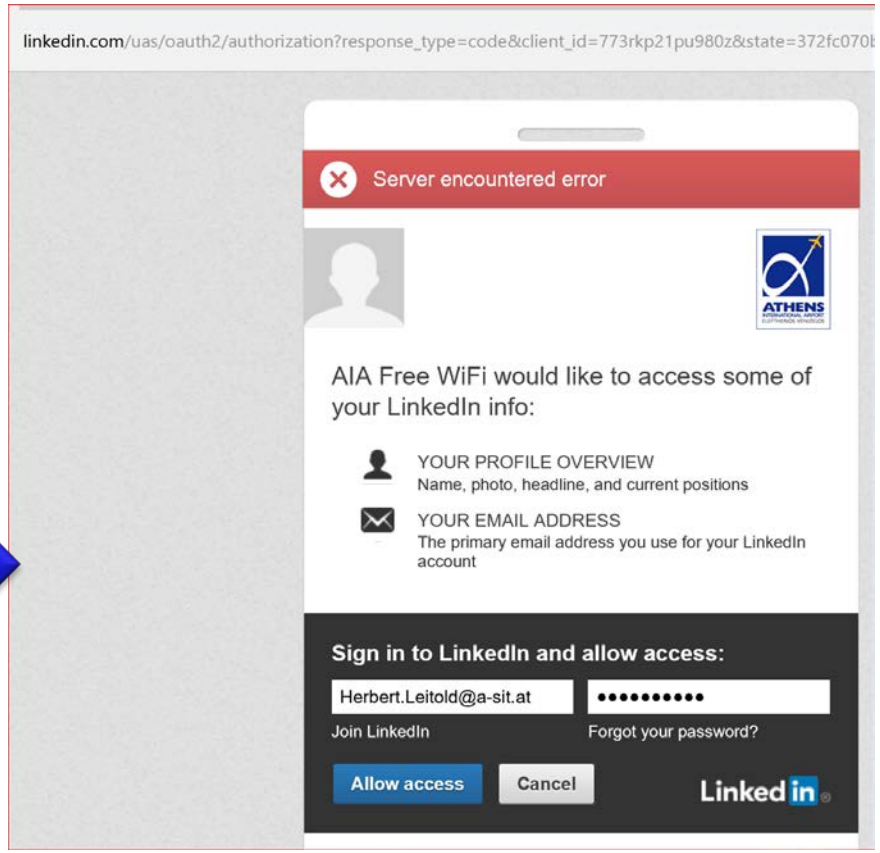
OAuth 2

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.

F12 DOM Explorer Konsole Debugger Netzwerk Leistung Speicher Emulation Experimente

Inhaltstyp

Suchen (STRG+F)

Name / Pfad	Protokol	Methode	Ergebnis / Beschreibung	Inhaltstyp	Empfangen	Zeit	Initiator / Typ
WizTempConnect.ashx?social=3&_=1469984277478 http://portal.wiz.athensairport.gr/handlers/	HTTP	GET	200 OK	text/html	122 B	250,69 ms	parsedElement
authorization?response_type=code&client_id=773rkp21pu980z&... https://www.linkedin.com/uas/oauth2/	HTTPS	GET	302 Found			6,04 s	document
validate?code=AQTeaMY4vCX9f56tb-_pXh0uHGHfK841raaQzaUg... http://portal.wiz.athensairport.gr/Social/	HTTP	GET	302 Found	text/html	167 B	1,37 s	document
cc1dbcec315c42e89f06c26d9dacc978 http://portal.wiz.athensairport.gr/Social/Connected/	HTTP	GET	200 OK	text/html	1,23 KB	33,45 ms	document
site?v=0-ezLmUmVnweEKURjS2TURYqqVLexOegk8L7OPDVPA81 http://portal.wiz.athensairport.gr/style/	HTTP	GET	200 OK	text/css	(aus dem Cache)	0 s	
jquery?v=gkWyJthHPtwkFjvHuNinBjchIfwLwc_KbE-H26J2kAI1 http://portal.wiz.athensairport.gr/bundles/	HTTP	GET	200 OK	text/javascript	(aus dem Cache)	0 s	

Header Text Parameter Cookies Zeiten

Anforderungs-URL: https://www.linkedin.com/uas/oauth2/authorization?response_type=code

Anforderungsmethode: GET

Statuscode: 302 / Found

Anforderungsheader

Accept: text/html, application/xhtml+xml, image/jxr, */*

Accept-Encoding: gzip, deflate

Accept-Language: de-LU, de-AT; q=0.8, de; q=0.6, en-GB; q=0.4, en; q=0.2

Connection: Keep-Alive

Cookie: bscookie=v=1&201607272041531bb28a13-f676-492d-8407-fc0f3f557010AQE

Host: www.linkedin.com

Header Text Parameter Cookies Zeiten

client_id: 773rkp21pu980z

redirect_uri: http://portal.wiz.athensairport.gr/Social/validate

response_type: code

scope: r_emailaddress

state: 30a06aa9d2d5d441692961245c46669e5

Header Text Parameter Cookies Zeiten

Anforderungs-URL: https://www.linkedin.com/uas/oau...

Anforderungsmethode: GET

Statuscode: 302 / Found

Anforderungsheader

Accept: text/html, application/xhtml+xml, image/jxr, */*

Accept-Encoding: gzip, deflate

Accept-Language: de-LU, de-AT; q=0.8, de; q=0.6, en-...

Connection: Keep-Alive

Cookie: bscookie=v=1&201607272041531bb28a13-f6...

Host: www.linkedin.com

Referer: http://portal.wiz.athensairport.gr/Welcome/lo...

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64...

Antwortheader

Cache-Control: no-cache, no-store

Connection: keep-alive

OAuth | Process Flow

```
+--------+                                +---------------+
|        |--(A)- Authorization Request ->|   Resource    |
|        |                               |     Owner     |
|        |<-(B)-- Authorization Grant ---|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(C)-- Authorization Grant -->| Authorization |
| Client |                               |     Server    |
|        |<-(D)----- Access Token -------|               |
|        |                               +---------------+
|        |
|        |                               +---------------+
|        |--(E)----- Access Token ------>|    Resource   |
|        |                               |     Server    |
|        |<-(F)--- Protected Resource ---|               |
+--------+                               +---------------+
```

Client ... Service Provider

Resource Owner ... User

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

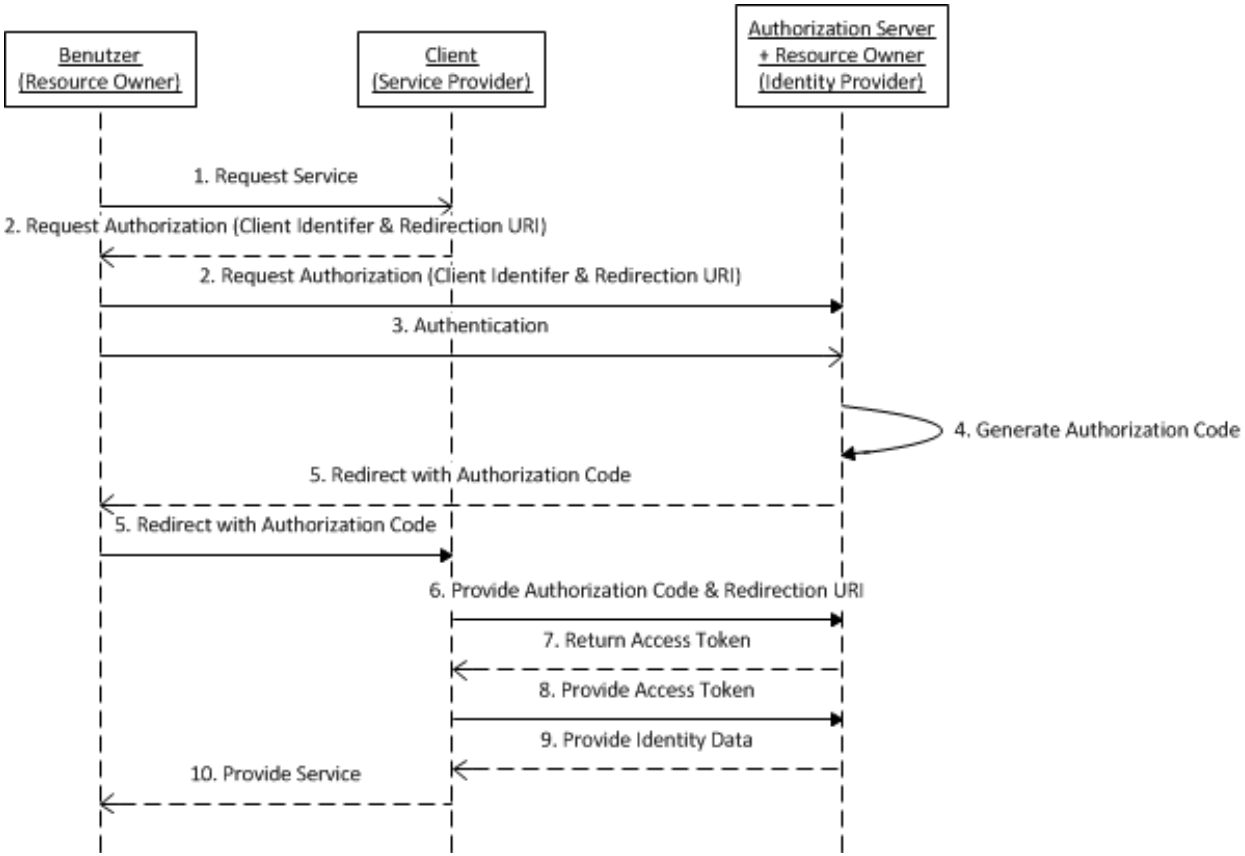
Resource Server ... Server that hosts the protected resource

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 SlAV32hkKG
```

- UserInfo request

```
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 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+LKwHPesHu10nr1fj4T8IAHX4IPiYR5OEDM
XtV1SvHfWI2XEBGh/MyJtk2qAFDT4OfgIneNk8hYPjcwNb8MwMME+tIR97snFMzkXI5tHSKB8LzGIPq+K2A0c06AX2LJiT8xaDscJTqqeaub4zIm6haZ1LZX0qMH2jFJVJAfYbV2BhdSs6aseTLSp+k2rIPJqvpds8PBN26I8KYb
k/bwQIZ0frSSo//f+q2cw==</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:KeyValue>
        <ds:RSAKeyValue>
<ds:Modulus>nEPzKMh3TovnfBnTyv+TMYFsGep8UiI7iNbfVyfLoBfqRdeGDOk4es2qWkgB6az+kM/9)s2H06m4
pjEY7/RIjd0IMWqgi8eqdjiIMmbFQykkYYQhIZbvi8KqoBcCKzj5N3GY4qh8A5qN4y85Q3sZj23T
iiIY1rphE+ZTOHCm6CKeRso9jj409YHP1xAXFvt1Yx2TA1uuagxOmL75OC/hr7gcUm0tmuKiSeq
+TO4VZw2Q7K7YESZ1WkiBoGZi4cHdcBfKnVrGNtyxi6UkjWxXRJSU9aNLs5QxsE6iFwCvFoIO+IU
cWxfHqOGbRtAcRUb4fk+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**


```
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
  Destination="https://demo.egiz.gv.at/demologin-pvp2-sso/secure/saml-acs/action"
  InResponseTo="_e3ace02d8006290189f8f48bdfc49441"Version="2.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">MOA-ID 2.0 Demo IDP</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="">
        <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#">
            <ec:InclusiveNamespaces xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"
              PrefixList="xs"/>
          </ds:Transform>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>XCBFTSFEpAMyygG5c8EBH9E1=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
<ds:SignatureValue>ymajo6Ar3F1Lo43CG63UJqbKjTHqxe54BwqBCOqdVJYjgzfDPkJeeZwbWAbTZ2o1YyF2ZR8RJmdmIQV0UO+Bq6ioldBs6uDE4djdgr2xDCdnoNjOvFZaeMecaWI0FFagrmWTWy5sDVdzfyoT6LSezJBt1aipBzyg2vcsBCLIWetUzQMHH4LCDJymwe+12980L34ZO+Rg40fhBTk8BzJmodBKHvdMKkFrcrf5ECB8RyB/EAupAZ3wdkqphvBRFTwovmwpS
wdNqgDqVtfkJ3vvA9NoeDYQEsDzqaSY2S0CcVPPkFUy/Y7bu06TRqBpaBaV88N/kMCFTw== </ds:SignatureValue>
    <ds:KeyInfo>
      <ds:KeyValue>
        <ds:RSAKeyValue>                <ds:Modulus>mWWy07+hO2VoMxOHpzN3cjl2rL2e3BczNkowmG+OpsR3LJpB0xbeRuzaeDPLseANfE9139PempsT
3cOKSSSB3bmvqZHDcf7EzBPkS2FYnvM+1HdBM0MGAdFWvdFsqzfHf4cbwRu6JJEKkimR1/X+M
vRPMD7/83fUJ8/DHZnyn25aZfd6Ug4RTjQQfBQhmHWzgcUSbQRaaG/KpaUJH6SWk7ZujWOs
3ubQzoo8bDqLcd5ly3bfcTCwCpdPSUPkNLg1F7AU+DHwem7Ero8D1DfHLNLg5v1dXbh6Byc
BCCpDS8FmAMBZbFD8TfDzNBwHyWQwAEw== </ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
      </ds:KeyValue>
    </ds:KeyInfo>
  </ds:Signature>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </saml2p:Status>
  <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_44cd66d4c7d28ff9f52f4023109f2baf" IssueInstant="2013-08-13T14:18:15.647Z" Version="2.0">
    <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">MOA-ID 2.0 Demo IDP</saml2:Issuer>
    <saml2:Subject>
      <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
        NameQualifier="urn:publicid:gv.at:cdid+BF*:BF/MA:Z0GFNraadWdbzeS4Rd5Y/c=</saml2:NameID>
      <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml2:SubjectConfirmationData InResponseTo="_e3ace02d8006290189f8f48bdfc49441"
          NotOnOrAfter="2013-08-13T14:38:15.647Z" Recipient="demologin-pvp2-sso/main/"/>
      </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2013-08-13T14:18:15.647Z"
      NotOnOrAfter="2013-08-13T14:38:15.647Z">
      <saml2:AudienceRestriction>
        <saml2:Audience>demologin-pvp2-sso/main/</saml2:Audience>
      </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2013-08-13T14:18:15.636Z"
      SessionIndex="_459457fc05fd27884feb81e88b09cdf">
      <saml2:AuthnContext>          <saml2:AuthnContextClassRef>http://www.stork.gov.eu/1.0/citizenQAALevel/4</saml2:AuthnContextClassRef>
      </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
      <saml2:Attribute FriendlyName="PVP-VERSION" Name="urn:oid:1.2.40.0.10.2.1.1.261.10"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:type="xs:string">2.2</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="PRINCIPAL-NAME" Name="urn:oid:1.2.40.0.10.2.1.1.261.20"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:type="xs:string">Mustermann</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="BPK" Name="urn:oid:1.2.40.0.10.2.1.1.149"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="xs:string">/BF:BA+Z0GFNraadWdbzeS4Rd5Y/c=</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="SID-SECTOR-FOR-IDENTIFIER"
        Name="urn:oid:1.2.40.0.10.2.1.1.261.34"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:type="xs:string">urn:publicid:gv.at:cdid+BF</saml2:AttributeValue>
      </saml2:Attribute>
    </saml2:AttributeStatement>
  </saml2:Assertion>
</saml2p:Response>
```


OpenID Connect

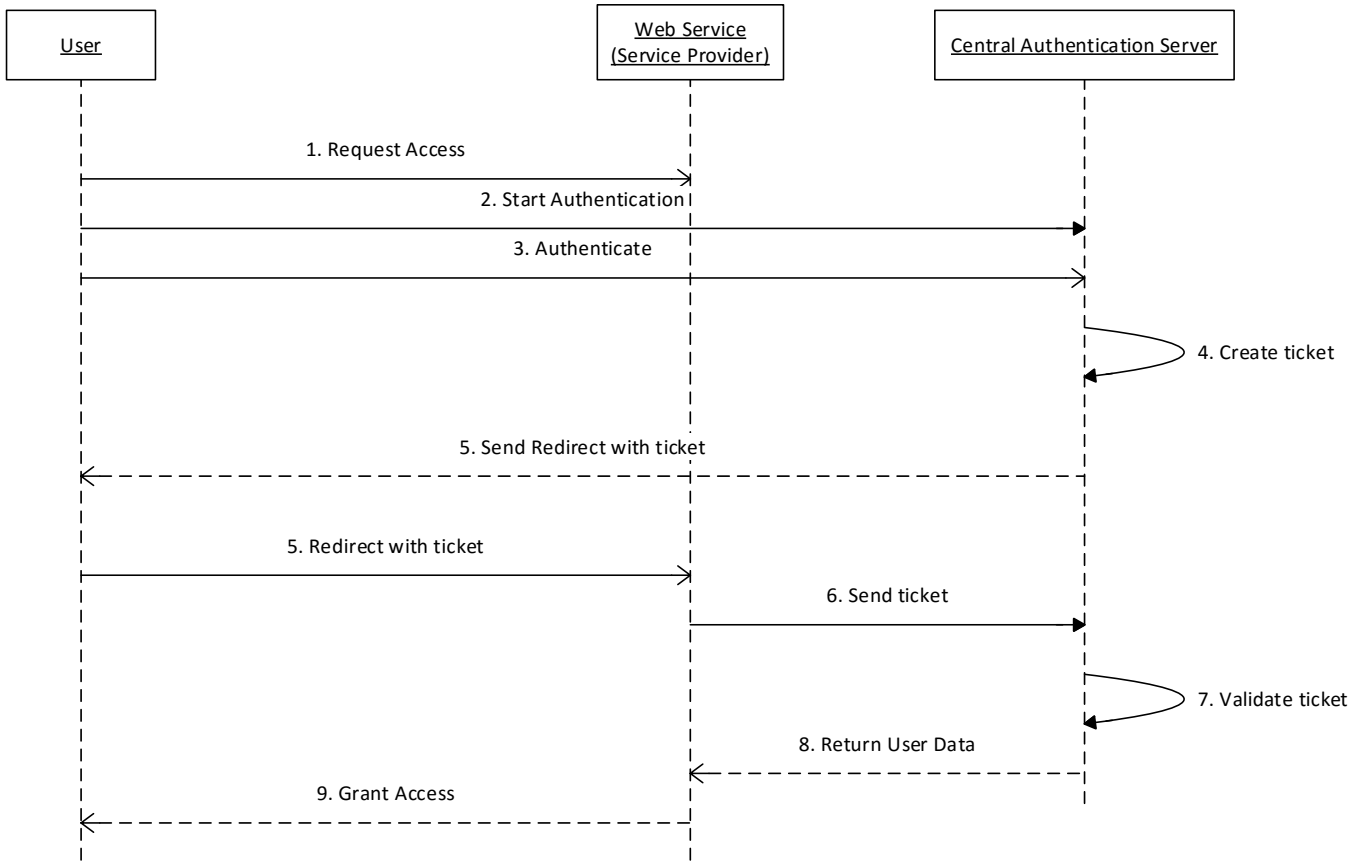

```
HTTP/1.1 200 OK
Content-Type:
application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache
{
"sub":"12345==",
"given_name":"Max",
"family_name":,"Mustermann"
"birthdate":,"01-01-1990"
"gender":,"M"
}
```

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
```

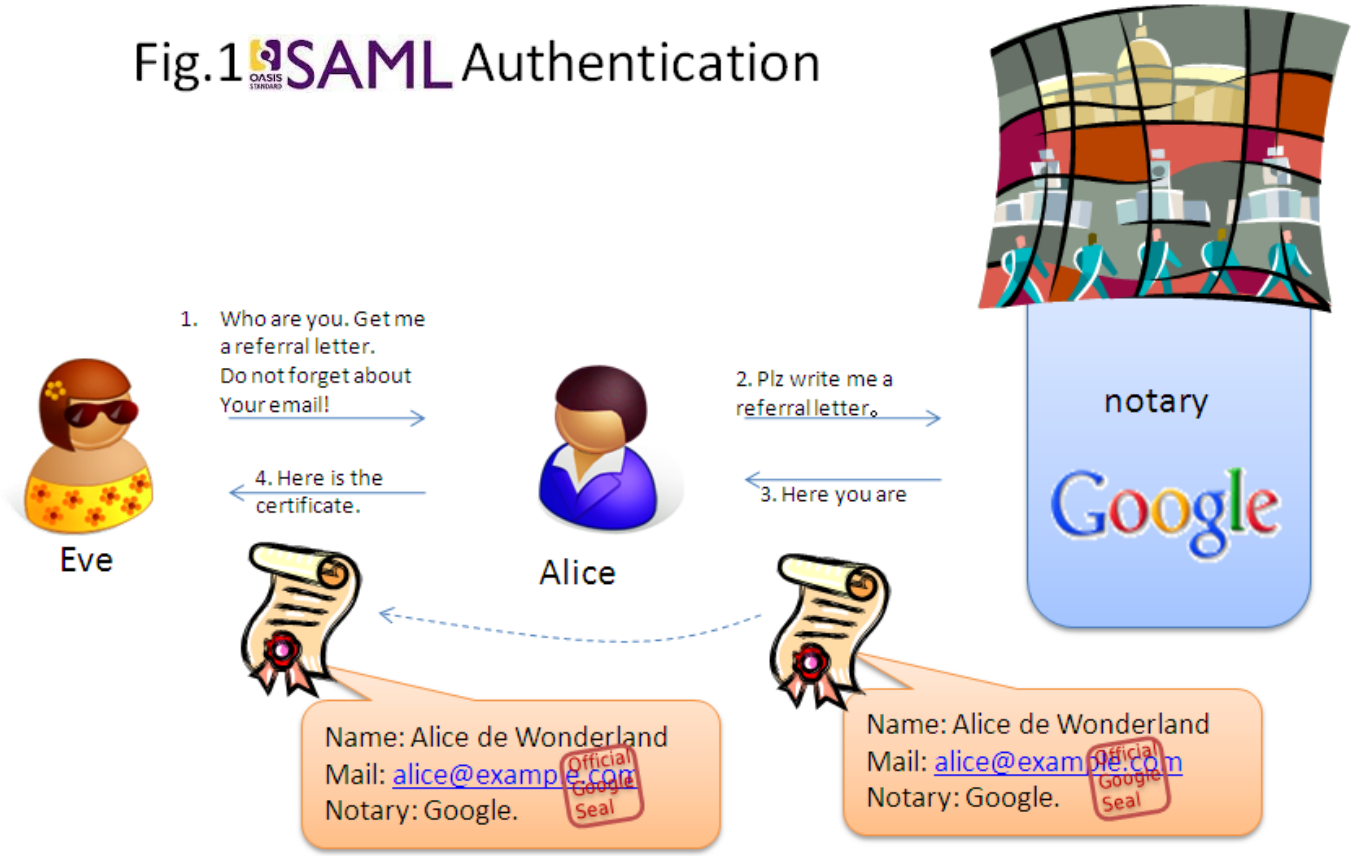
CAS 3.0

```
<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

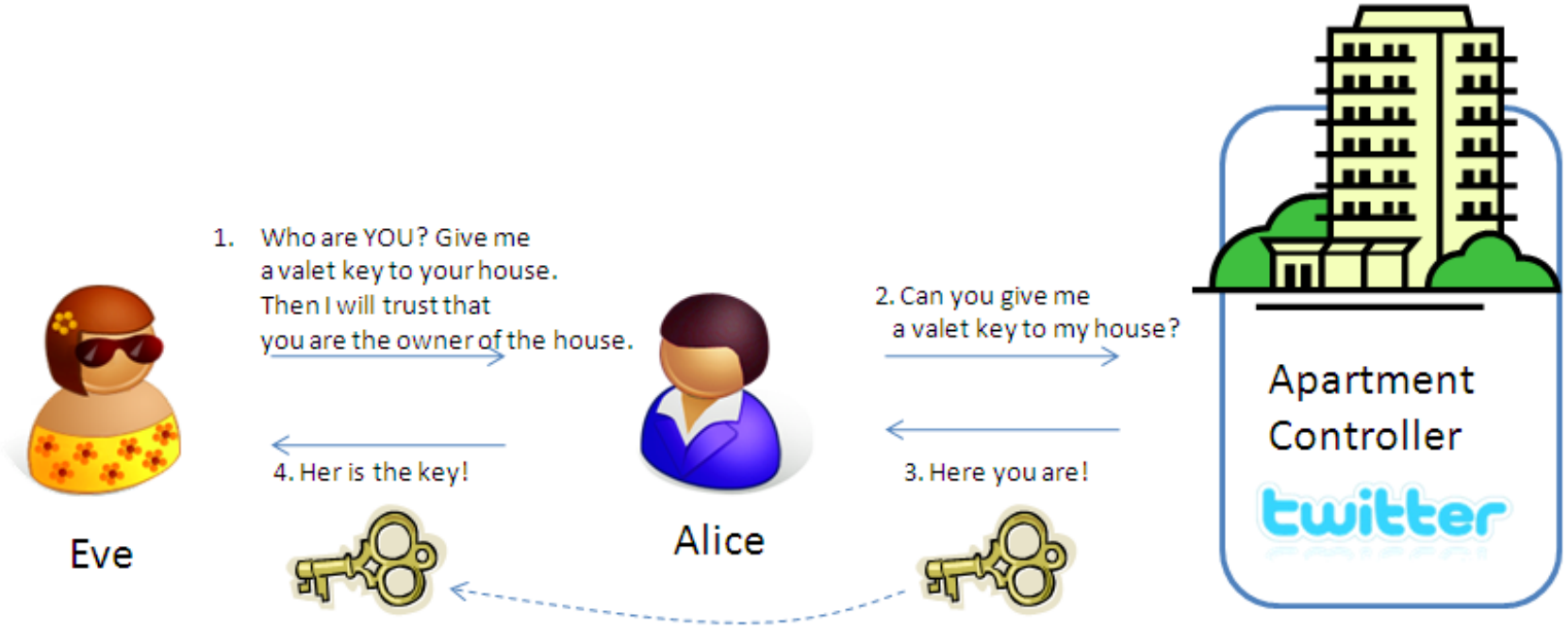
Summary



Ref: Sakimura

Summary

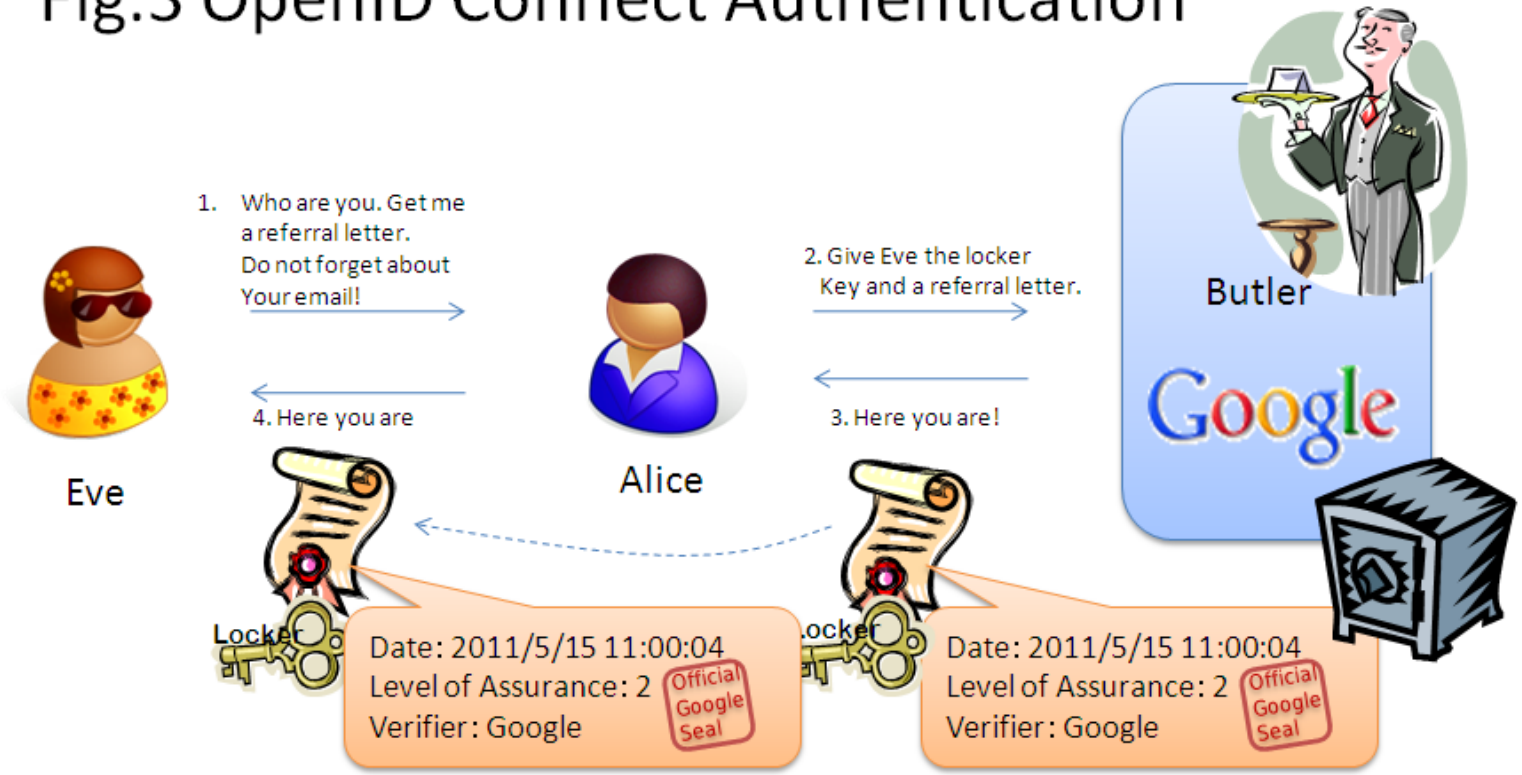
Fig.2 Pseudo-Authentication using OAuth



Ref: Sakimura

Summary

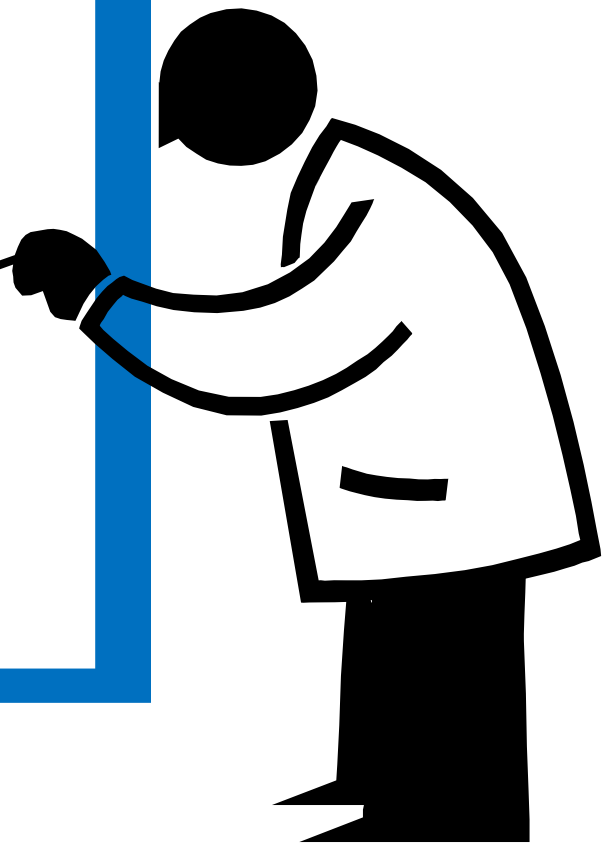
Fig.3 OpenID Connect Authentication



Ref: Sakimura

Contents

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



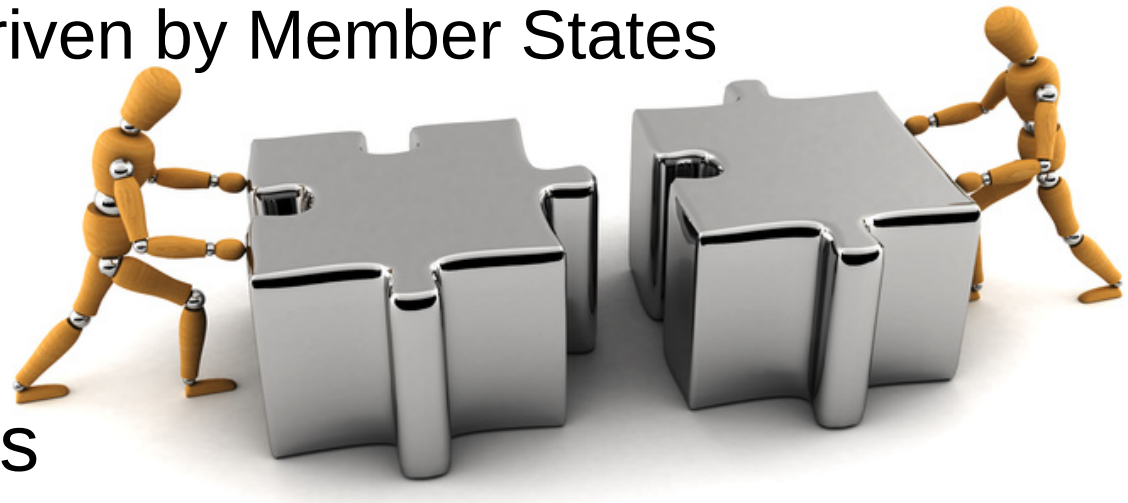
Single Digital Market?

- 13 million EU citizens work in another EU country
- 21 SMEs with significant international operations
- 120 mio. shop online, only 20 % buy in another EU state

- Cross-border administration examples
  - 600.000 citizens live in one EU MS and work in another
  - 350.000 per year engage in an marriage with a national of another MS
  - 180.000 students move to another MS (Erasmus / post-graduate degree)

EC's ICT Policy Support Programme

- Large Scale Pilots to support key policy areas
  - Focus on cross-border aspects
  - Pilots A: Driven by Member States



- STORK has been the LSP on eID interoperability

LSPs: MS cooperate in key policy areas

- Building Block Provision
- eID interoperability
- eHealth
- eJustice
- Services Directive
- eProcurement

SENS moving services forward.eu

STORK making access smarter.eu

epsos EUROPEAN PATIENTS SMART OPEN SERVICES making healthcare better.eu

eECODEX making justice faster.eu

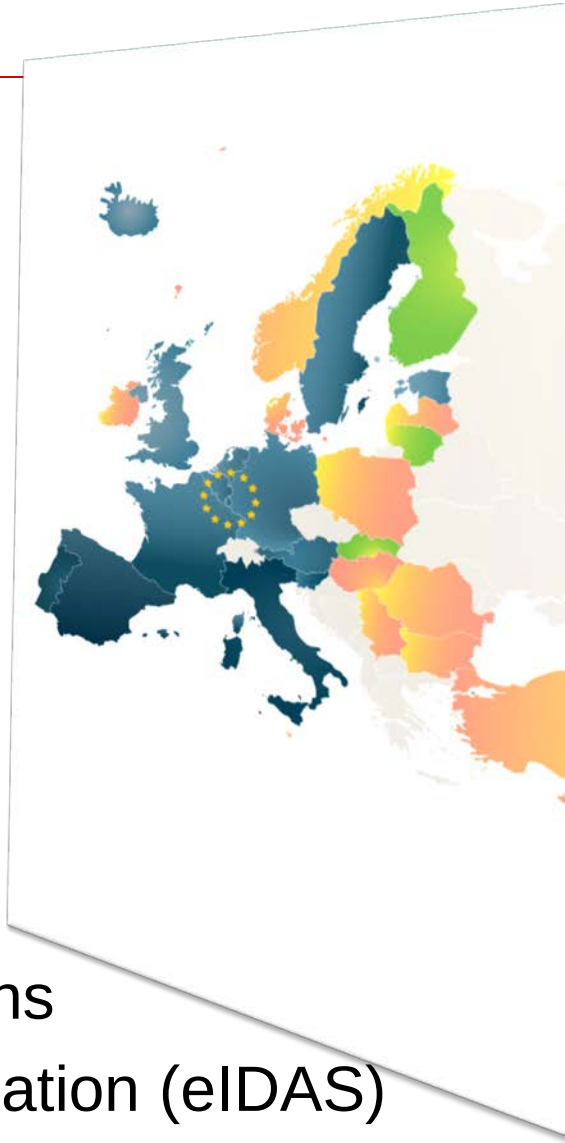
SPOCS making business easier.eu

PEPPOL PAN-EUROPEAN PUBLIC PROCUREMENT ONLINE making procurement better.eu

STORK making access smarter.eu

SECTION 7: STORK OVERVIEW

STORK Phase 1 Key-facts



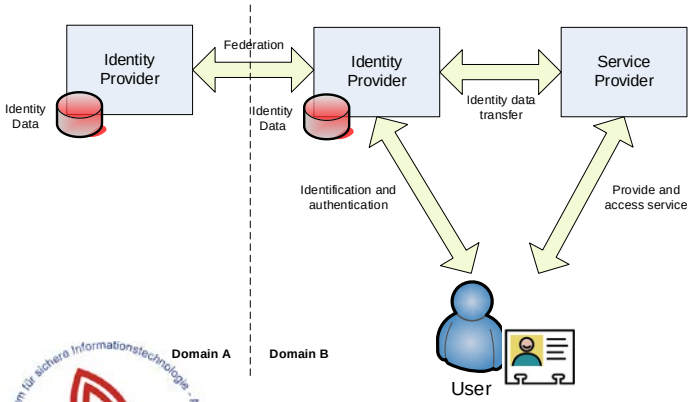
- Project than ran from 2008-2011
- National eID federation between
  - 18 MS
  - 100+ national eID token types
  - 6 pilots in production systems
- Resulted in
  - Open specifications (SAML 2 + QAA)
  - Open source reference implementations
  - Lessons learned as basis for EU legislation (eIDAS)

eID profile of 1st pilot phase (2010): MS situation is different

Country & credentials		Token Types			Relation to 1999/93/EC		Token Issuer	
	# of cred.	Smart card	mobile eID	soft.-certif.	qualified cert (signature-cert)	is a SSCD	public sector	private sector
Austria	3	yes	yes	-	all	all	yes	yes (all. qual.c.)
Belgium	1	yes	-	-	all	all	yes	-
Estonia	2	yes	yes	-	all	all	yes	-
Germany	1	yes	-	-	optional	all	yes	(opt. qual.certs.)
Finland	1	yes	-	-	qualified	all	yes	-
Iceland	2	yes	-	-	all	all	-	yes
Italy	2	yes	-	-	all	all	yes	yes (sig.-card)
Lithuania	1	yes	-	-	all	all	yes	-
Luxembourg	3	yes	yes	-	all	all	-	yes
Portugal	1	yes	-	-	all	all	yes	-
Slovenia	3	yes	-	yes	all	yes (QAA 4)	yes	yes
Spain	1+80	yes	-	yes	all	yes (QAA 4)	yes (QAA 3-4)	yes (QAA 3-4)
Sweden	12+	yes	yes	yes	-	no	yes	yes

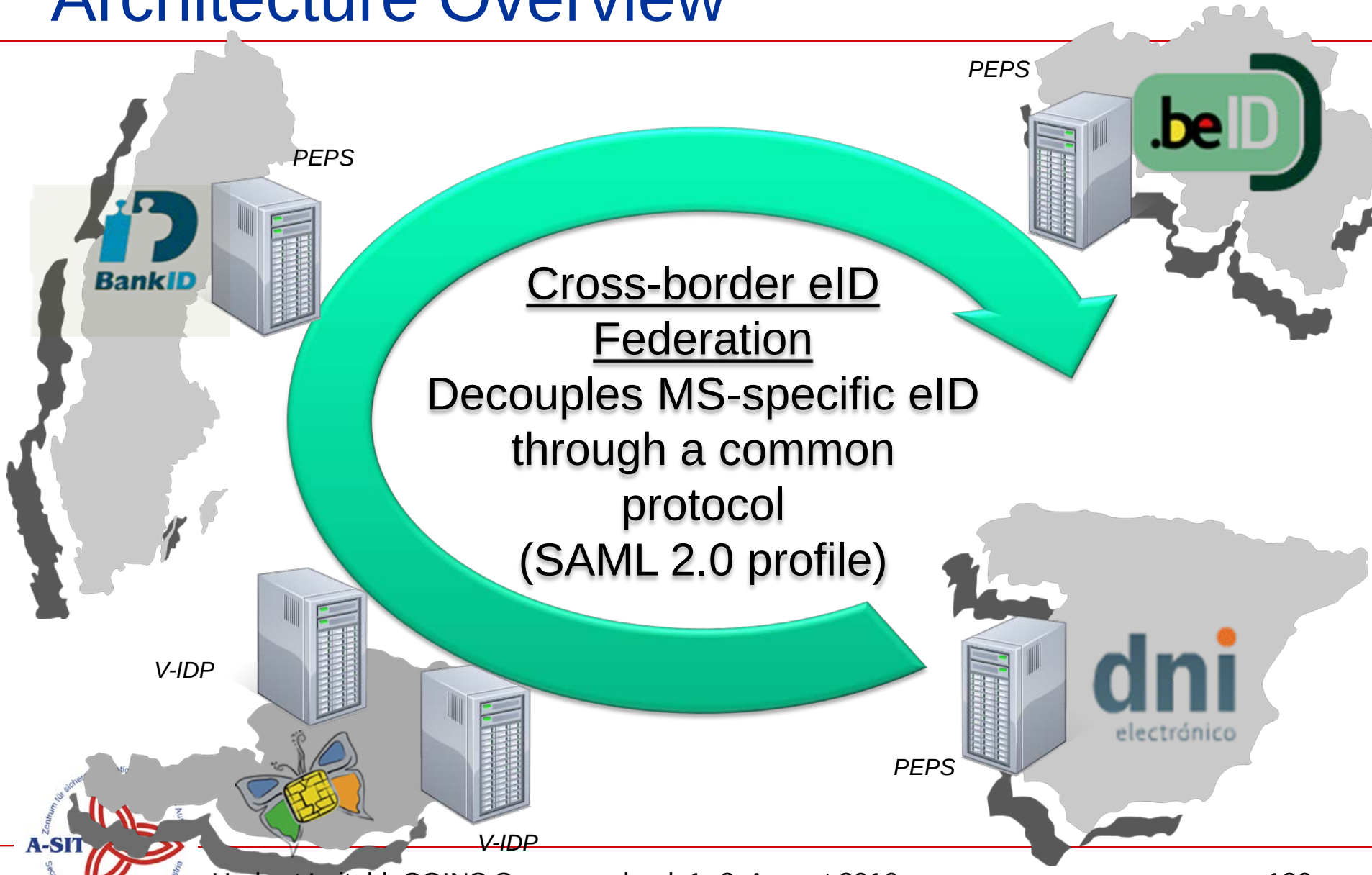
Overall principle

STORK **does not change** the MS eID, but builds interoperability **on top of it** (*eID federation*)



Note, however, that in several federation protocols each SP may do IdP discovery of all IdPs. Moreover they assume sort of a homogeneous situation on protocols/profiles. Both give organisational challenges and interfere with existing MS infrastructure.

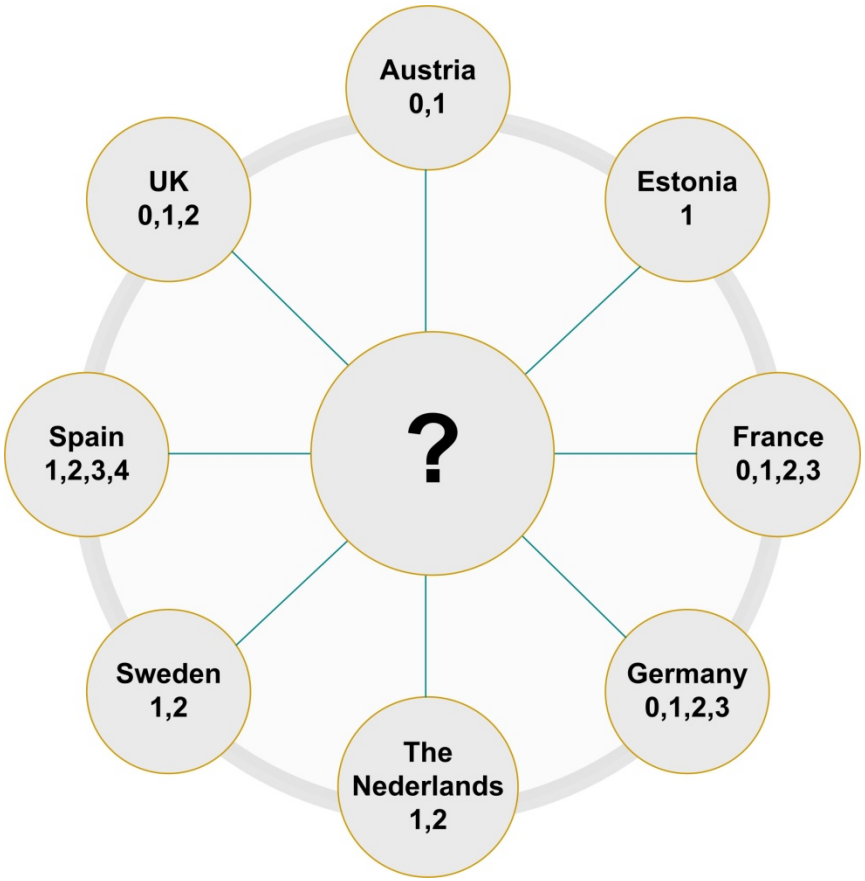
Architecture Overview



The pilots

- Six pilots live as “pioneering applications”
  - Online authentication
  - Safer Chat
  - Student Mobility
  - eDelivery
    - Affiliate
  - Change of Address
  - ECAS

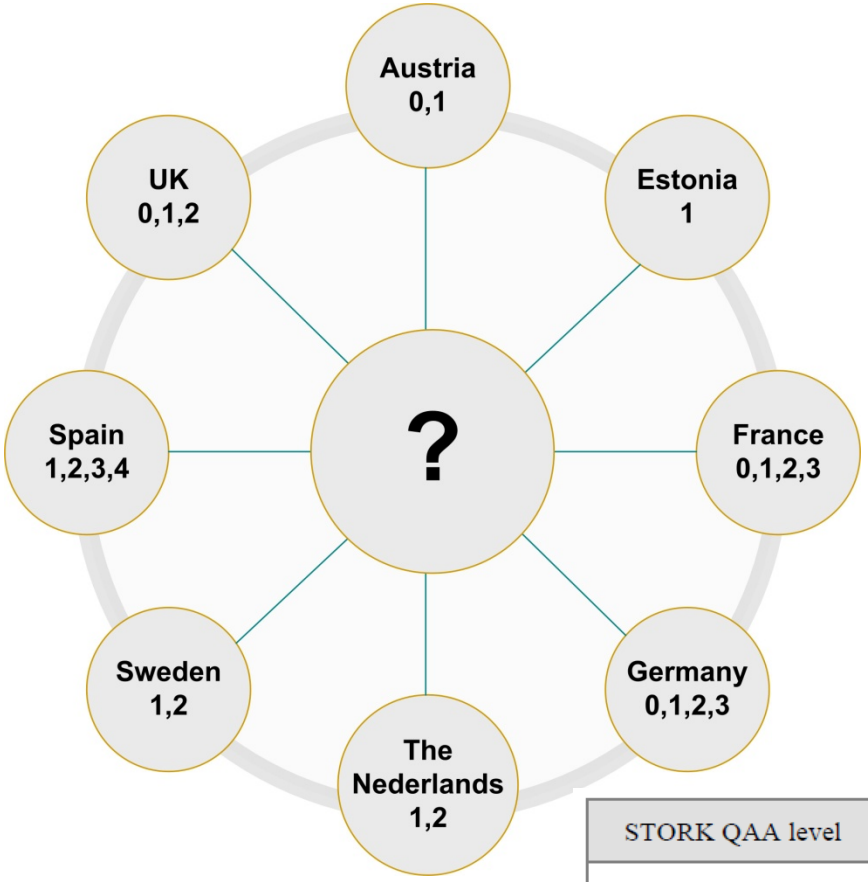
One problem tackled: Trust levels

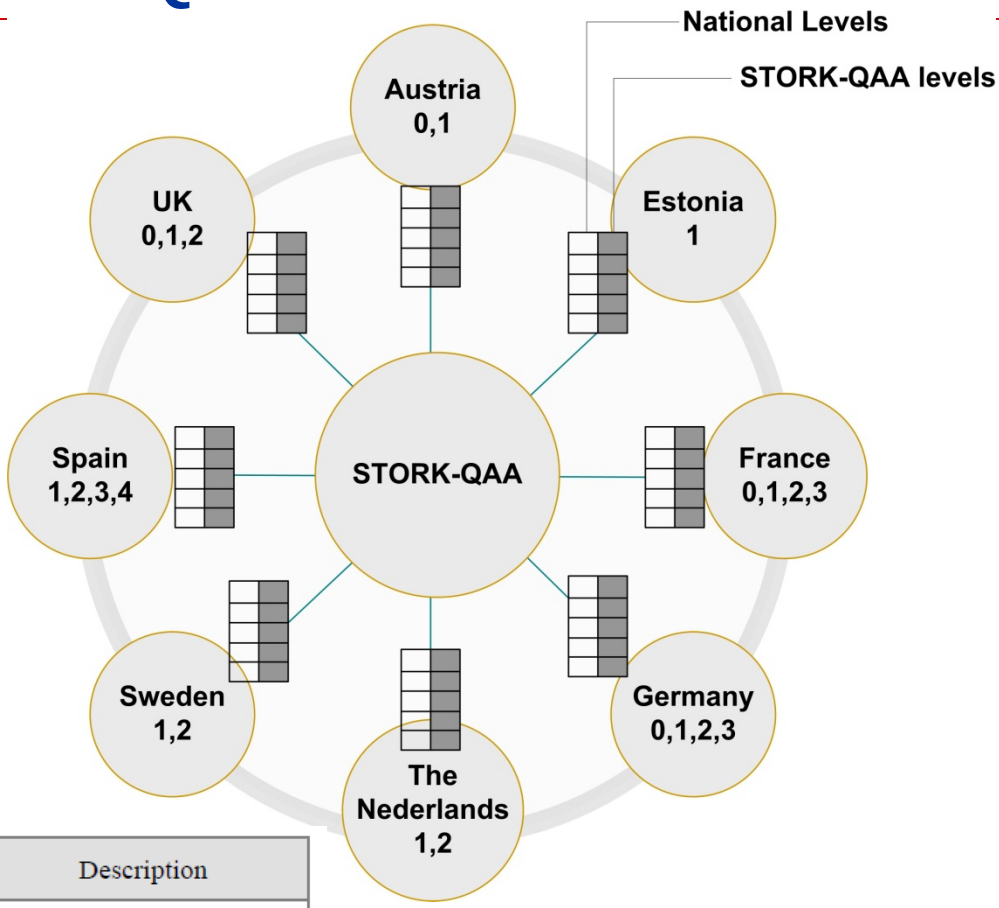


Different technologies and security levels:

- Smart cards
- Software certificates
- Mobile Phones
- Username-password

Approach: Mapping to QAA levels

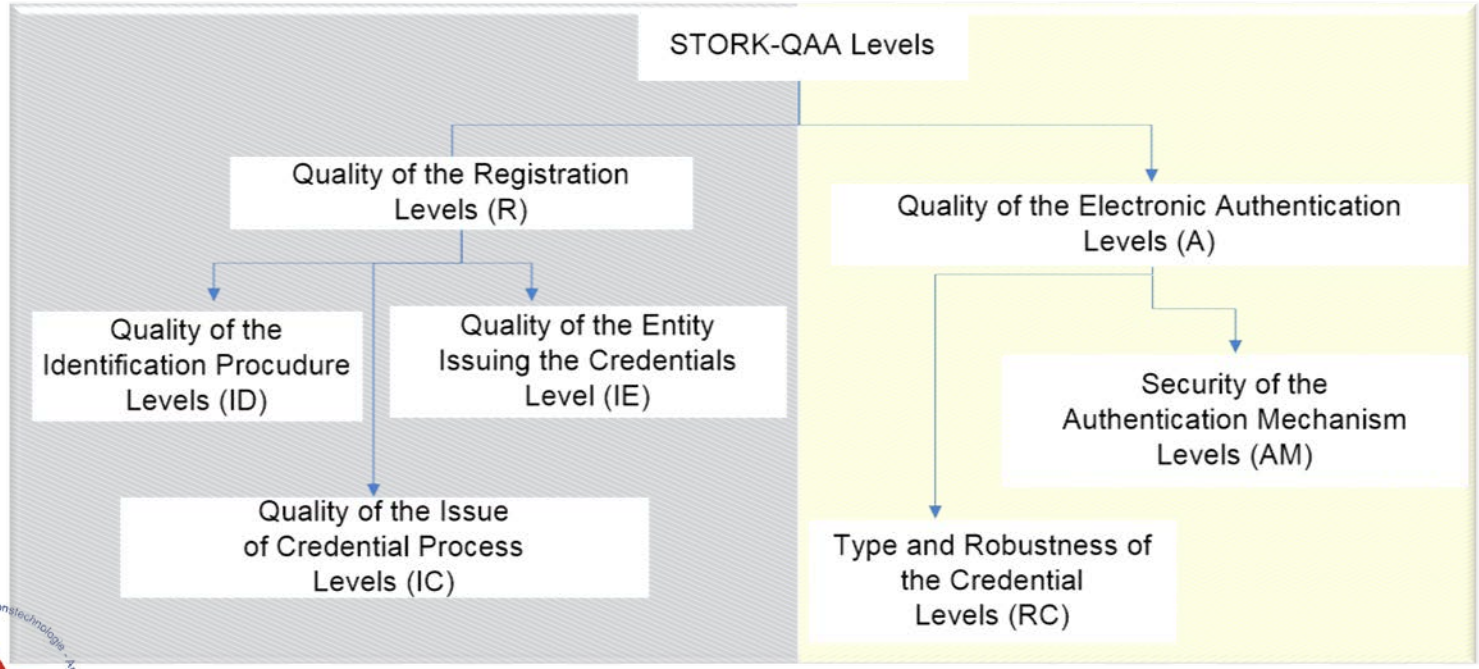




STORK QAA level	Description
1	No or minimal assurance
2	Low assurance
3	Substantial assurance
4	High assurance

QAA: Security - Assurance

- **Assurance**: grounds for confidence that a component meets the security requirements
- STORK QAA: registration and credential



SECTION 8: IMPLEMENTATION

STORK –Interoperability Models

One Interoperability Framework, Two Basic Models

STORK investigated and pilots two interoperability models:

1. **Decentralized *aka* Middleware (MW)**
2. **Centralized *aka* Pan-European Proxy Services (PEPS)**

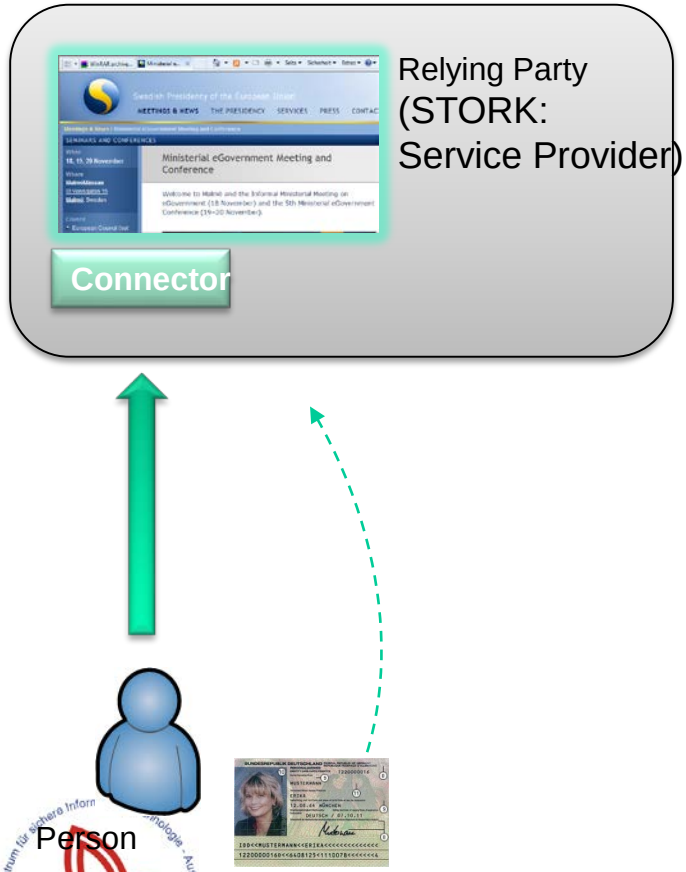
.. and combine them (*MW⇨MW, PEPS⇨PEPS, MW⇨PEPS, PEPS⇨MW*)

The common specifications have been designed so that major components operate on the same protocols, irrespective of the model or its combinations.

Direct vs. Indirect authentication

Replay from section 5

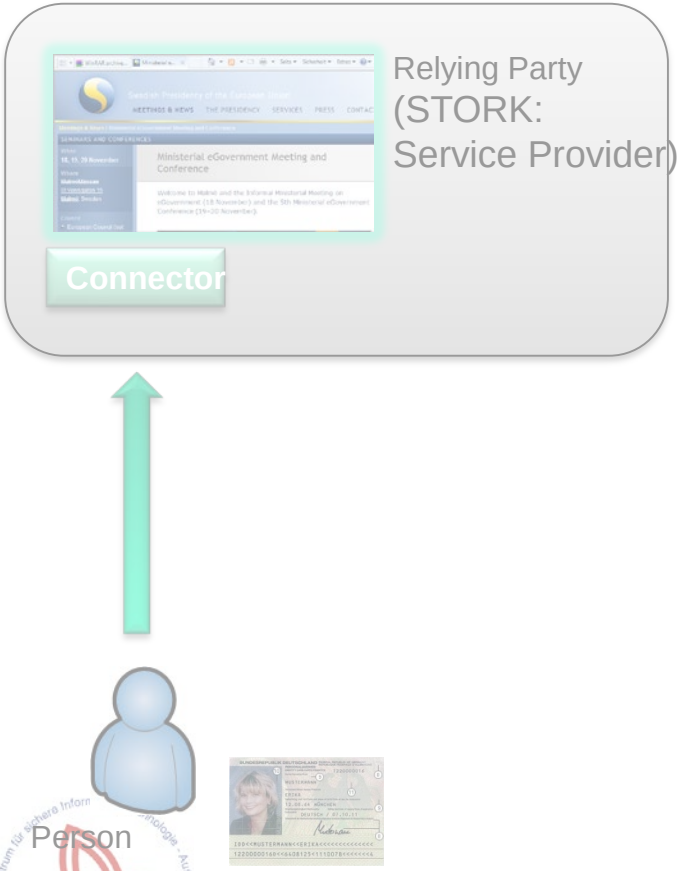
Direct Authentication



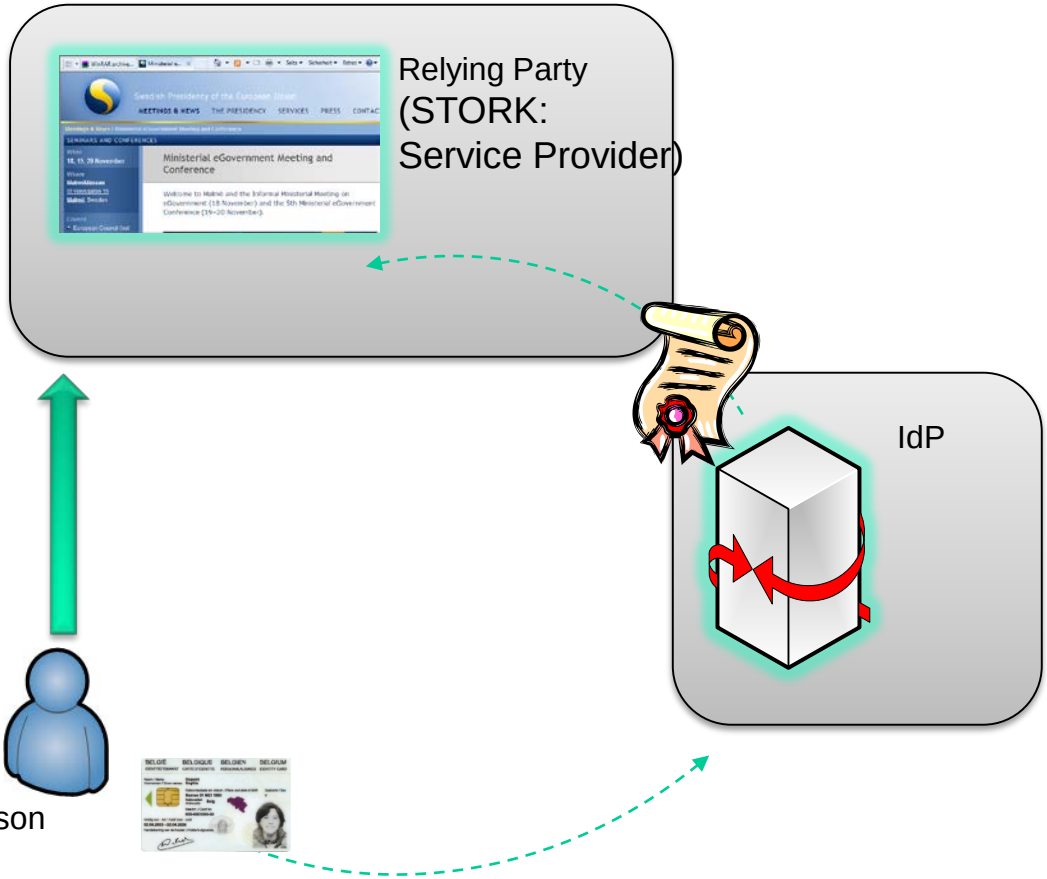
Direct vs. Indirect authentication

Replay from section 5

Direct Authentication



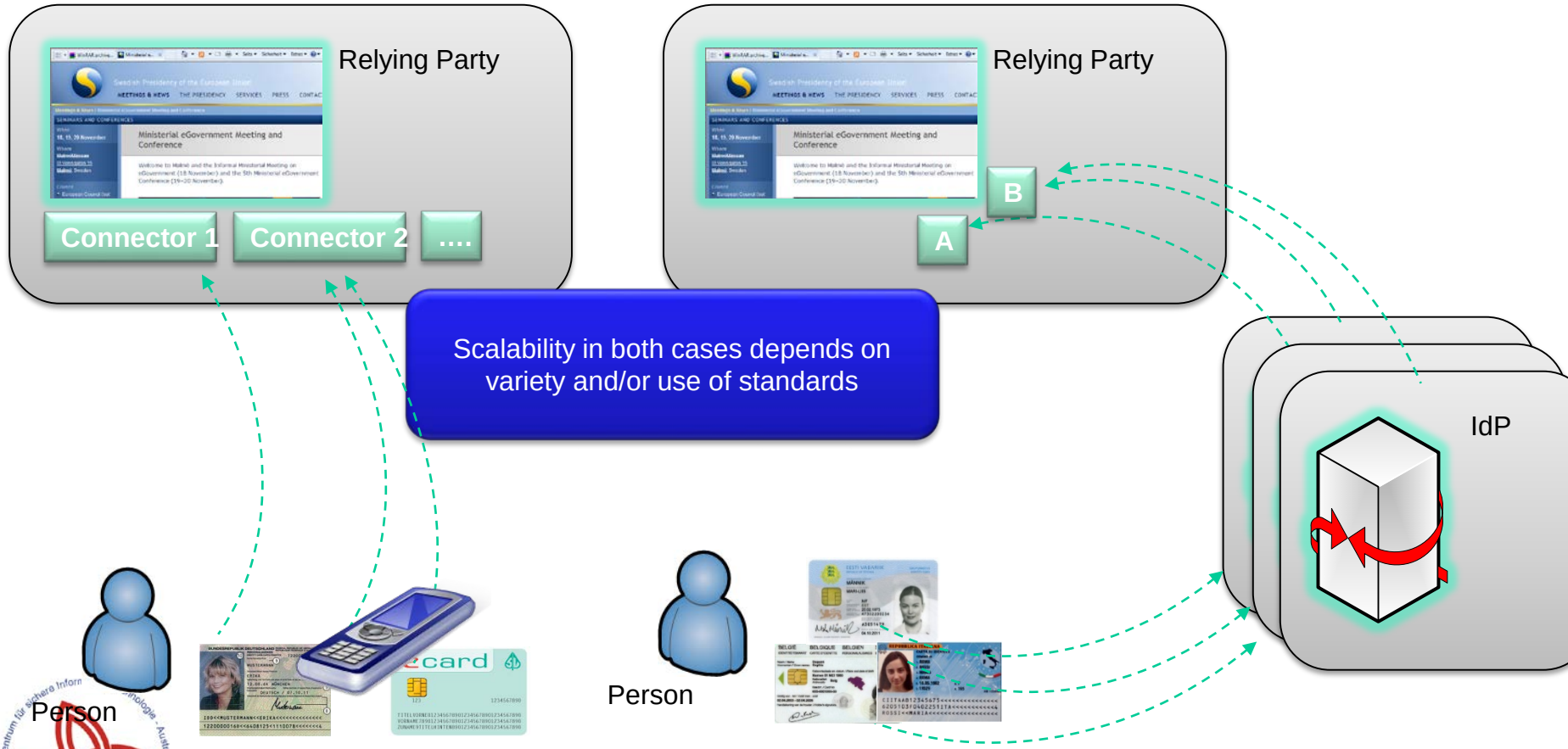
Indirect (IdP-based) Authentication



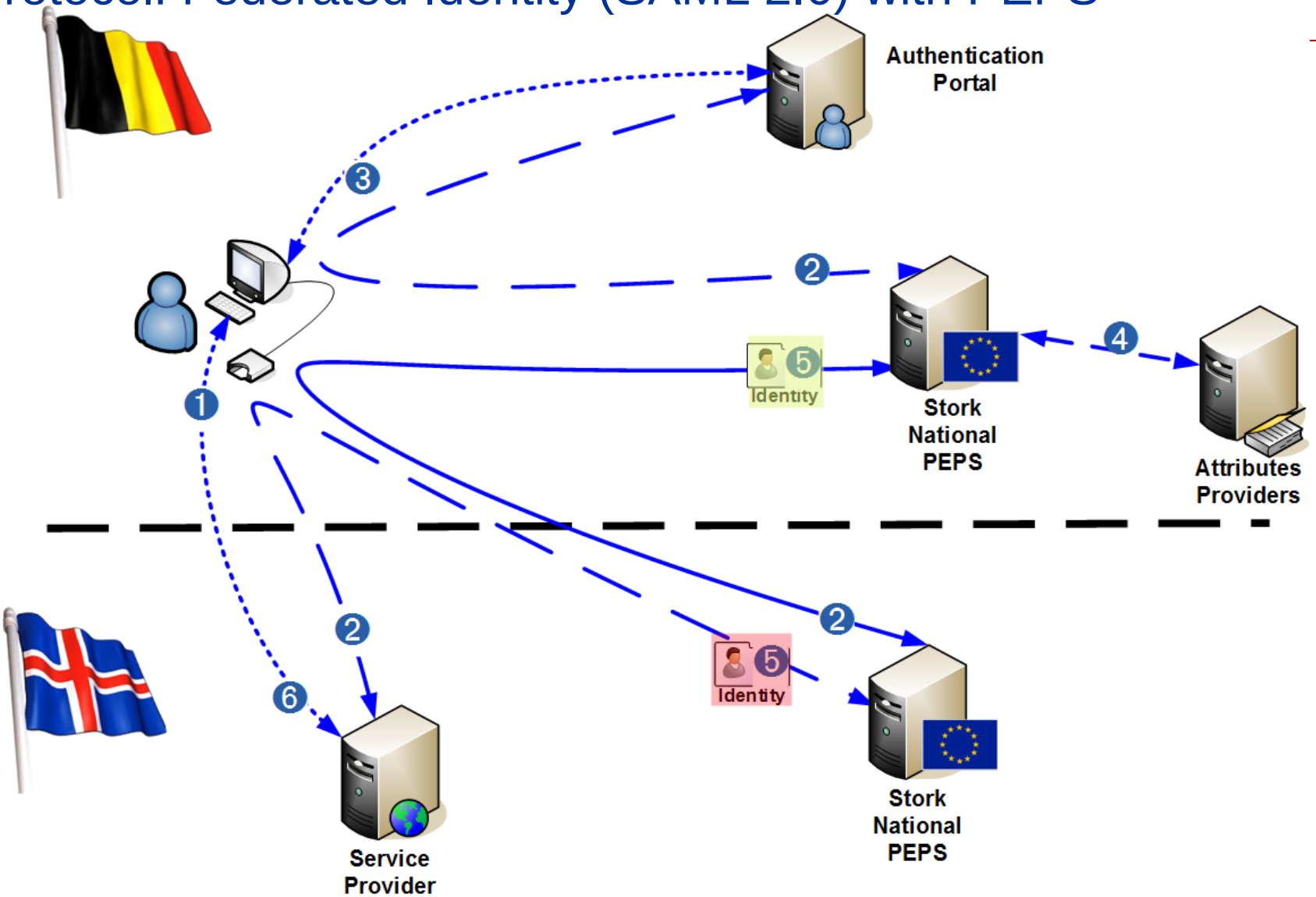
Direct vs. Indirect authentication

Replay from section 5

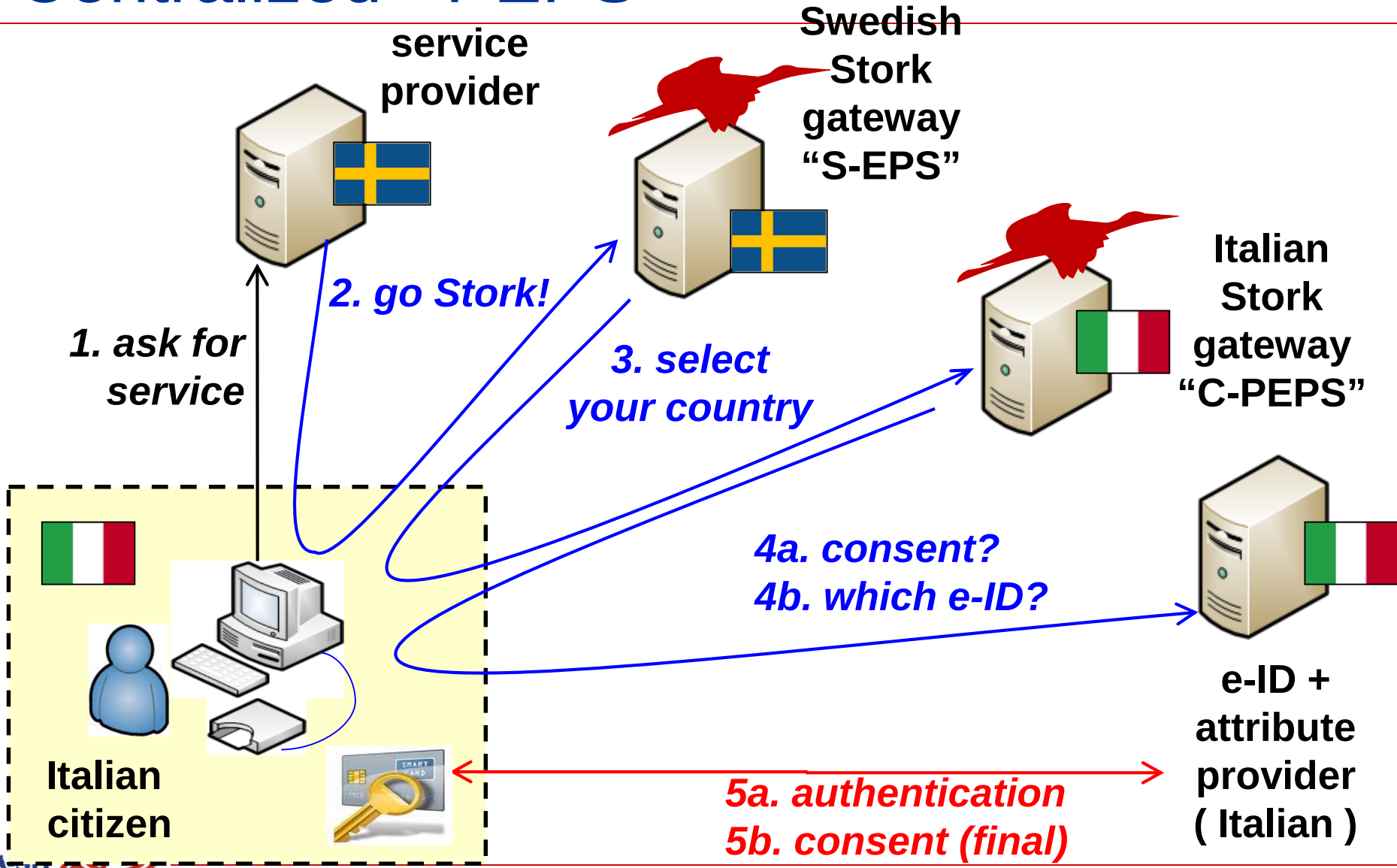
Direct Authentication | **Indirect (IdP-based) Authentication**



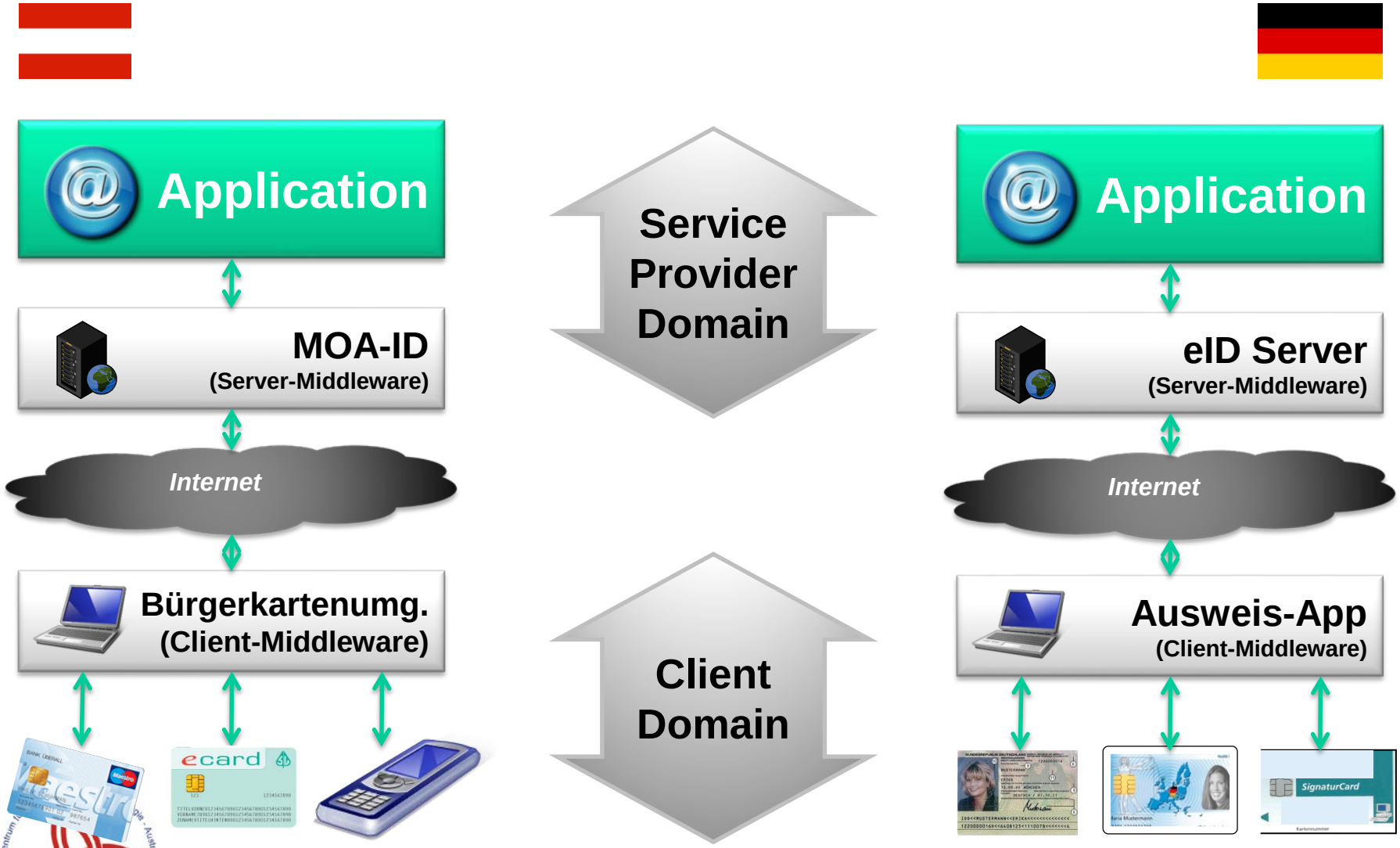
Protocol: Federated Identity (SAML 2.0) with PEPS



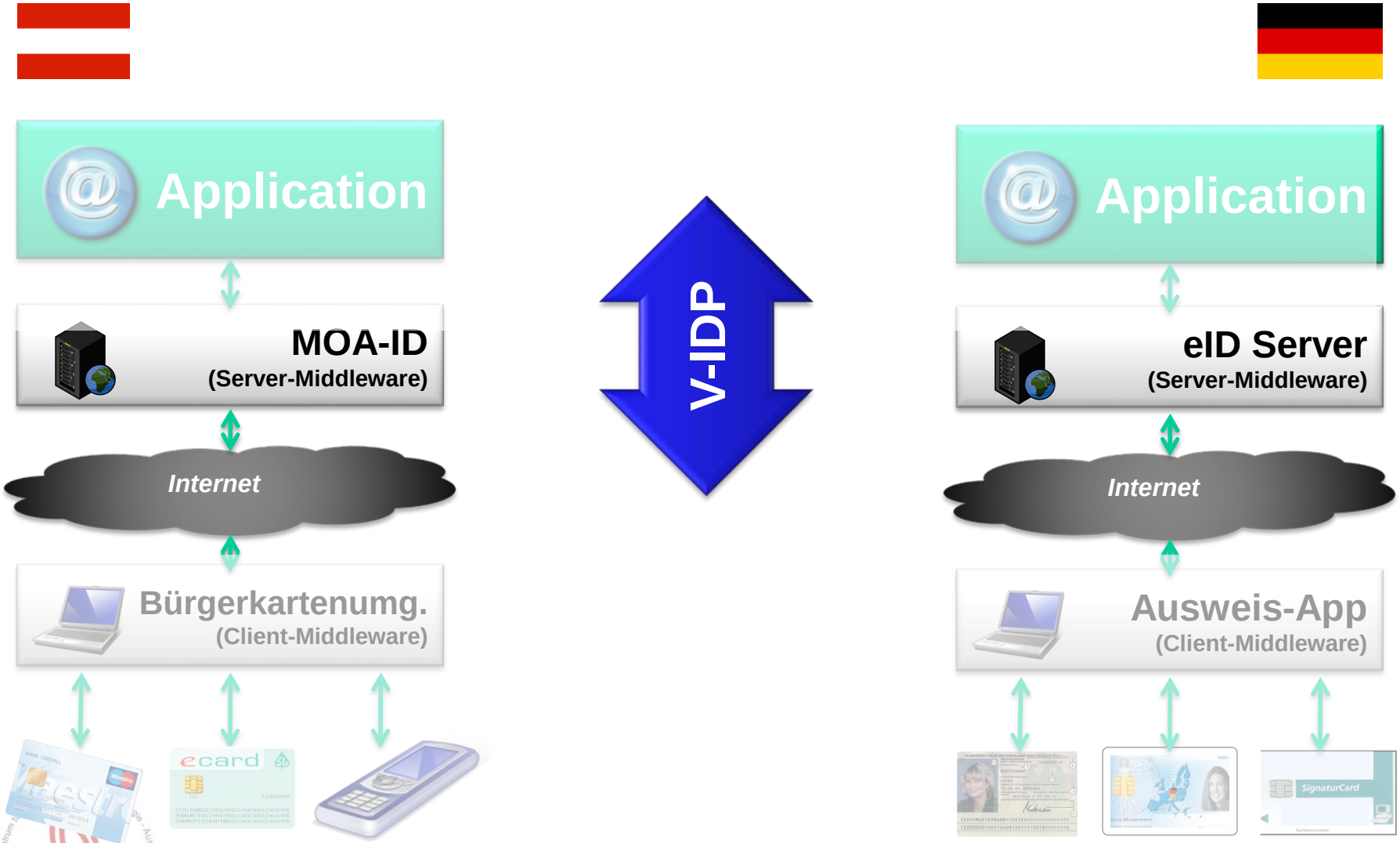
Centralized - PEPS



Decentralized – Middleware Approach



Decentralized – Common Middleware / Virtual-Identity Provider



PEPS Architecture

A PEPS routes between MS-specific eID-schemes and common protocols

<u>Two major parts</u>

- C-PEPS: The citizen authenticates to (can be through IdPs)
- S-PEPS: Provides assertion to relying party (service prov.)

Common MW architecture

The V-IDP is a component that routes MS-specific eID-schemes and common protocols

Common specifications and modules

- Common Specifications: SAML 2.0
  - √ Web SSO Profile; HTTP POST binding
  - √ Extensions for QAA, cross-border ID and attributes
- Open Source reference implementations
  - √ https://joinup.ec.europa.eu/software/stork/home

- Reference PEPS
  - Java 1.5
  - Application Servers - Web application
    - Tomcat 5/6
    - JBoss 5
    - Glassfish V3

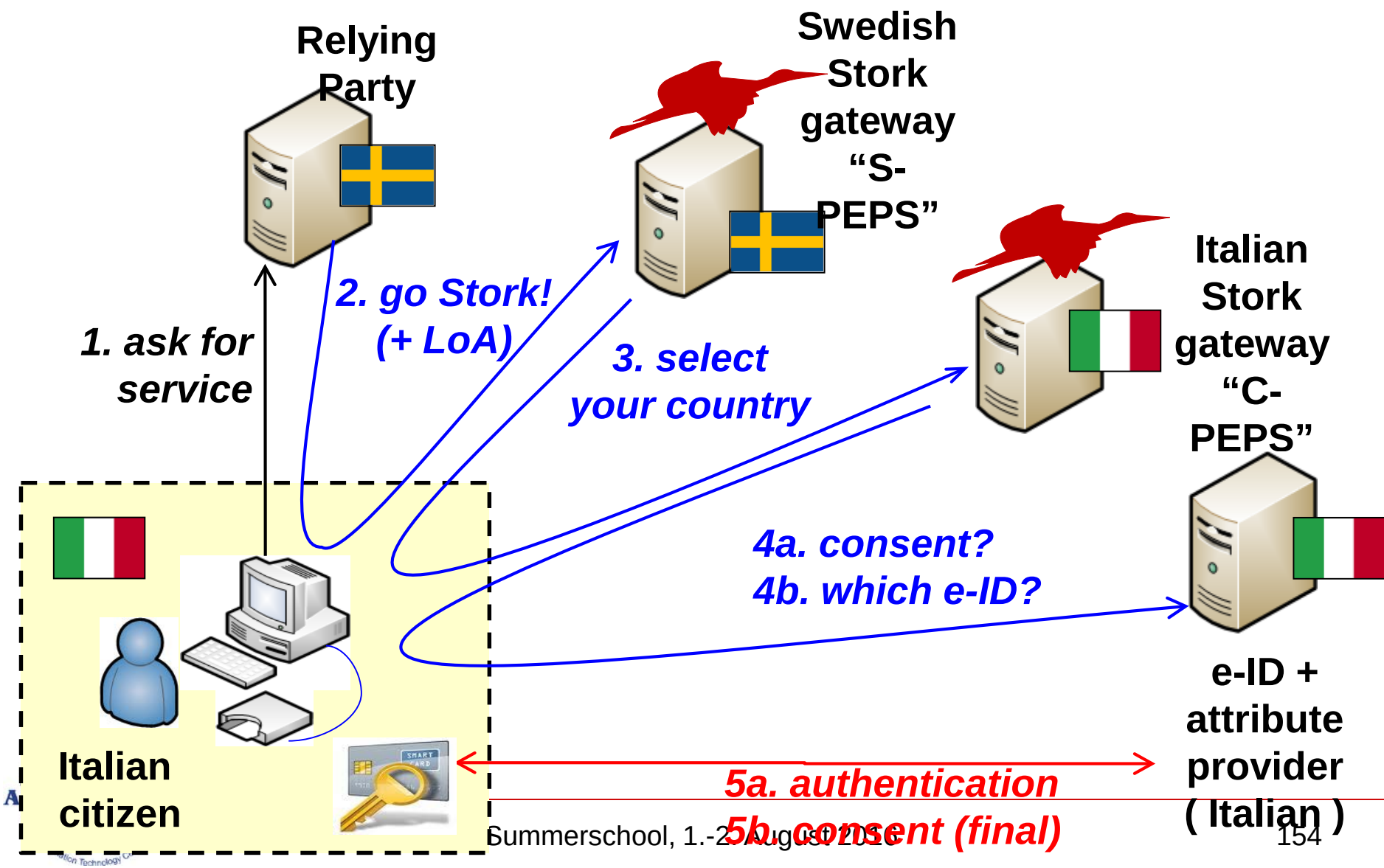
- Reference V-IDP
  - √ Java 1.5
  - √ Application Servers - Enterprise application
    - Glassfish V2
    - jboss
    - Weblogic

Common vs. MS-specific parts

- How to deal with existing MS infrastructure?
- How to cope with two models PEPS & MW?
  - (we'll call is centralized vs. decentralized in eIDAS)
- How to integrate?

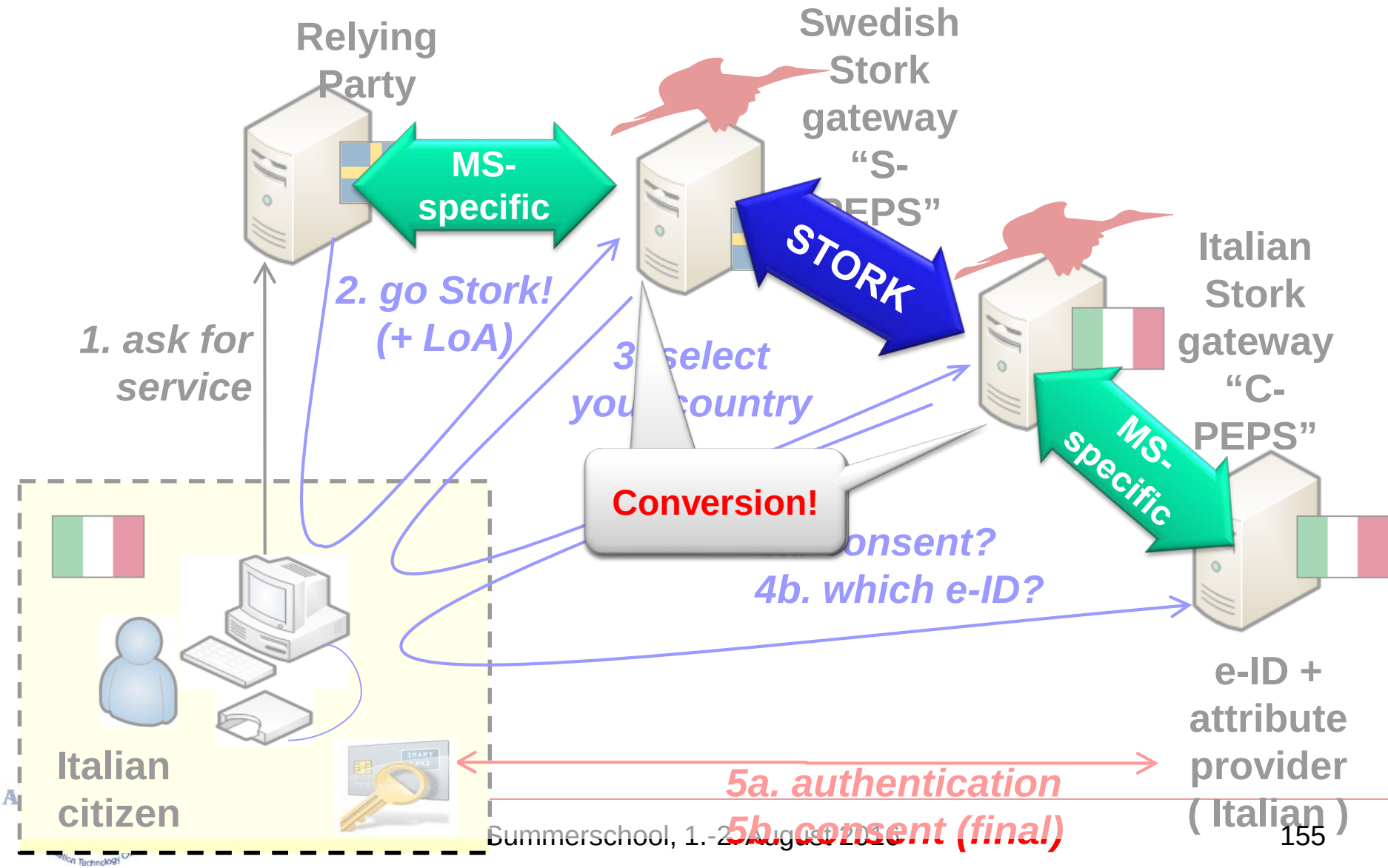
Centralized – PEPS Process

common STORK and MS-specific parts



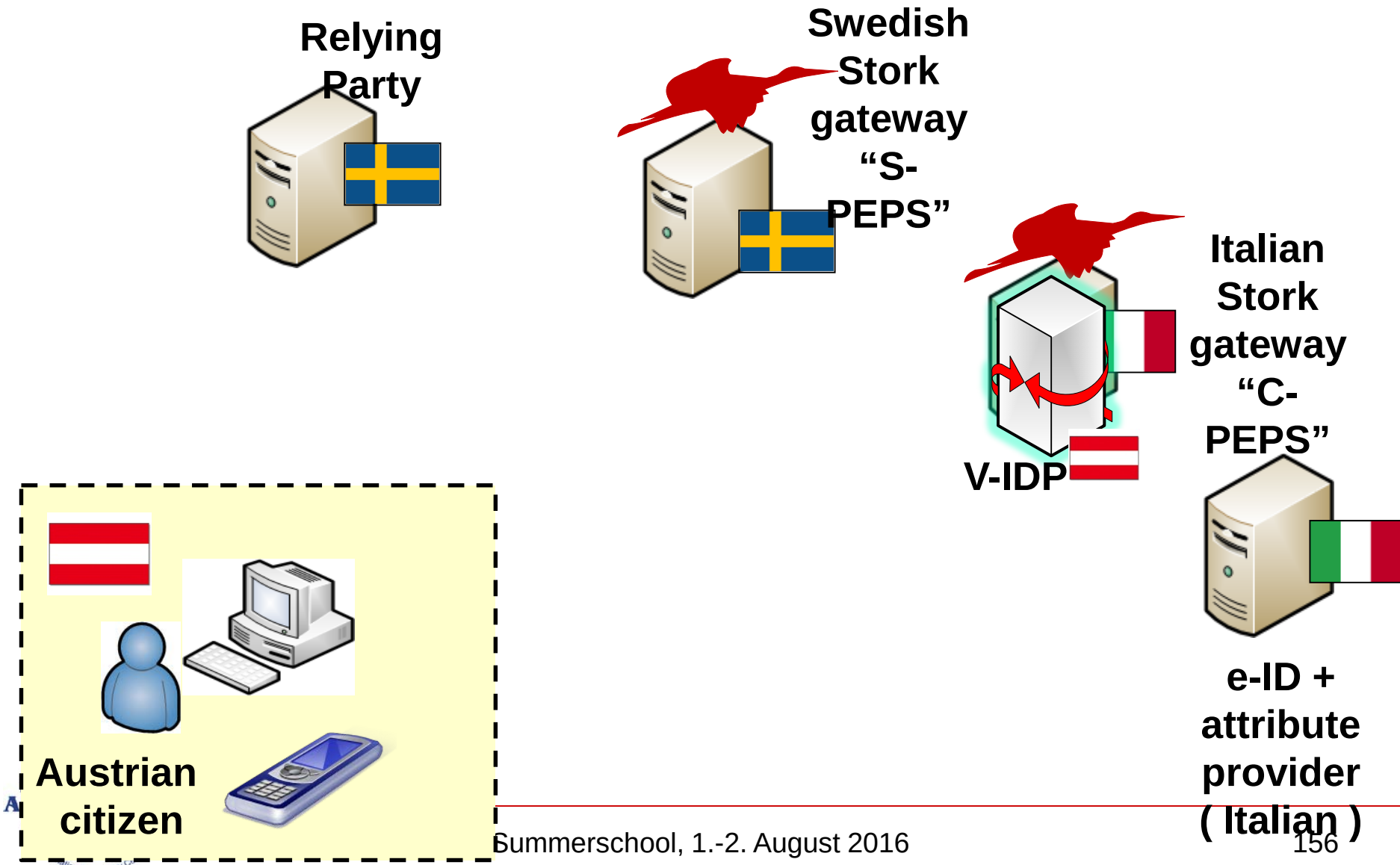
Centralized – PEPS Process

common STORK and MS-specific parts



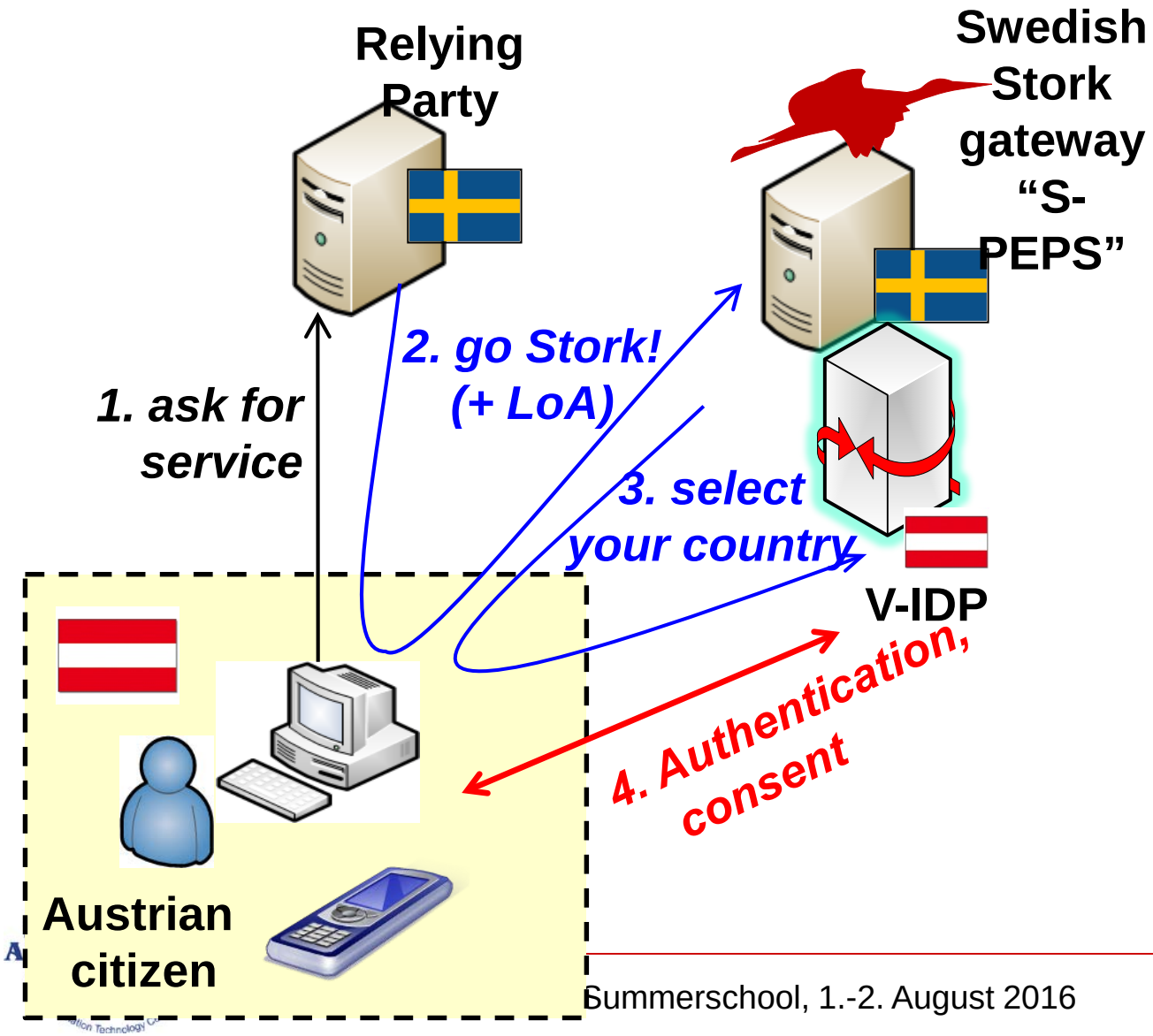
PEPS-VIDP Process

Austrian accessing Swedish Relying Party



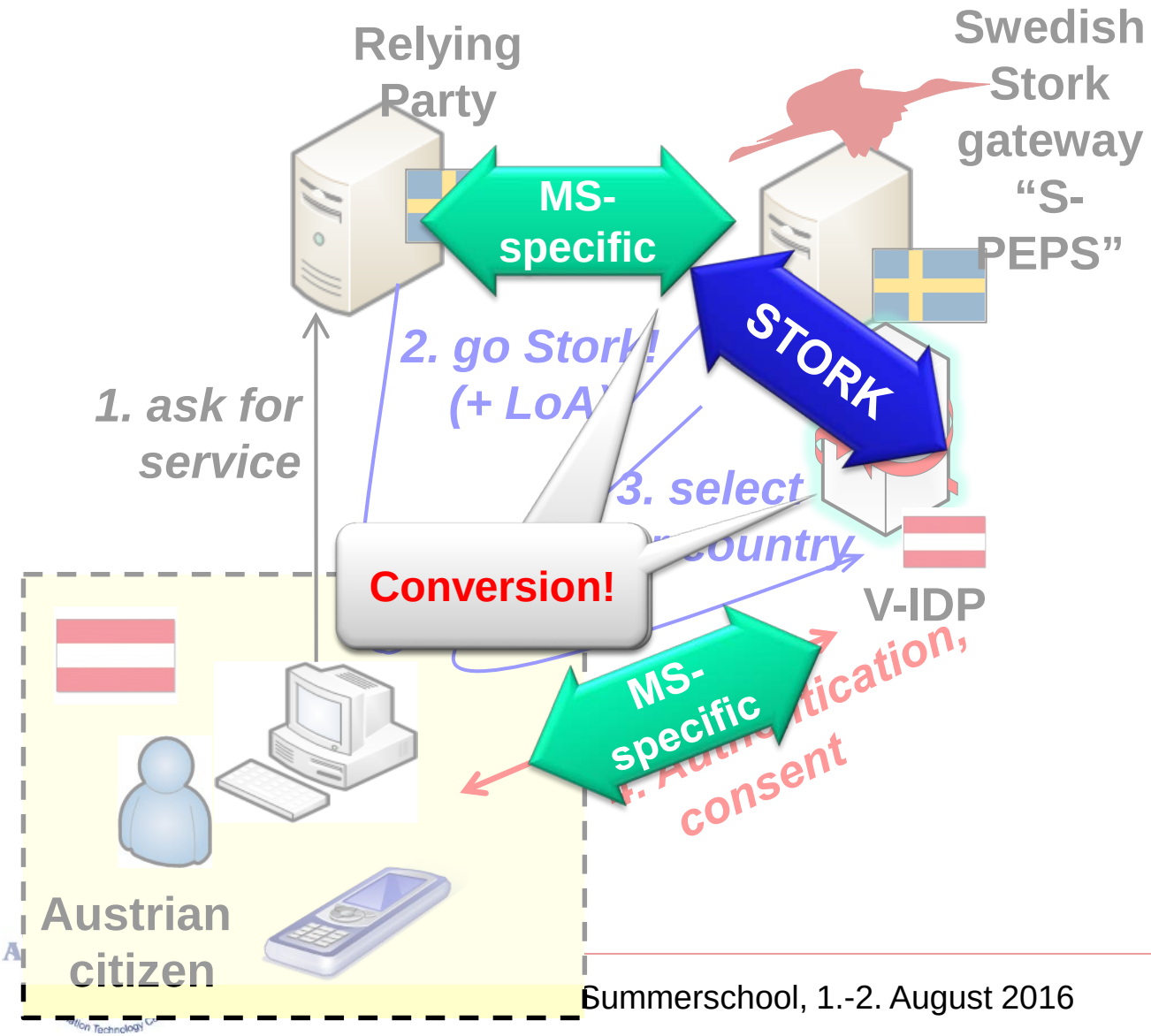
PEPS-VIDP Process

Austrian accessing Swedish Relying Party



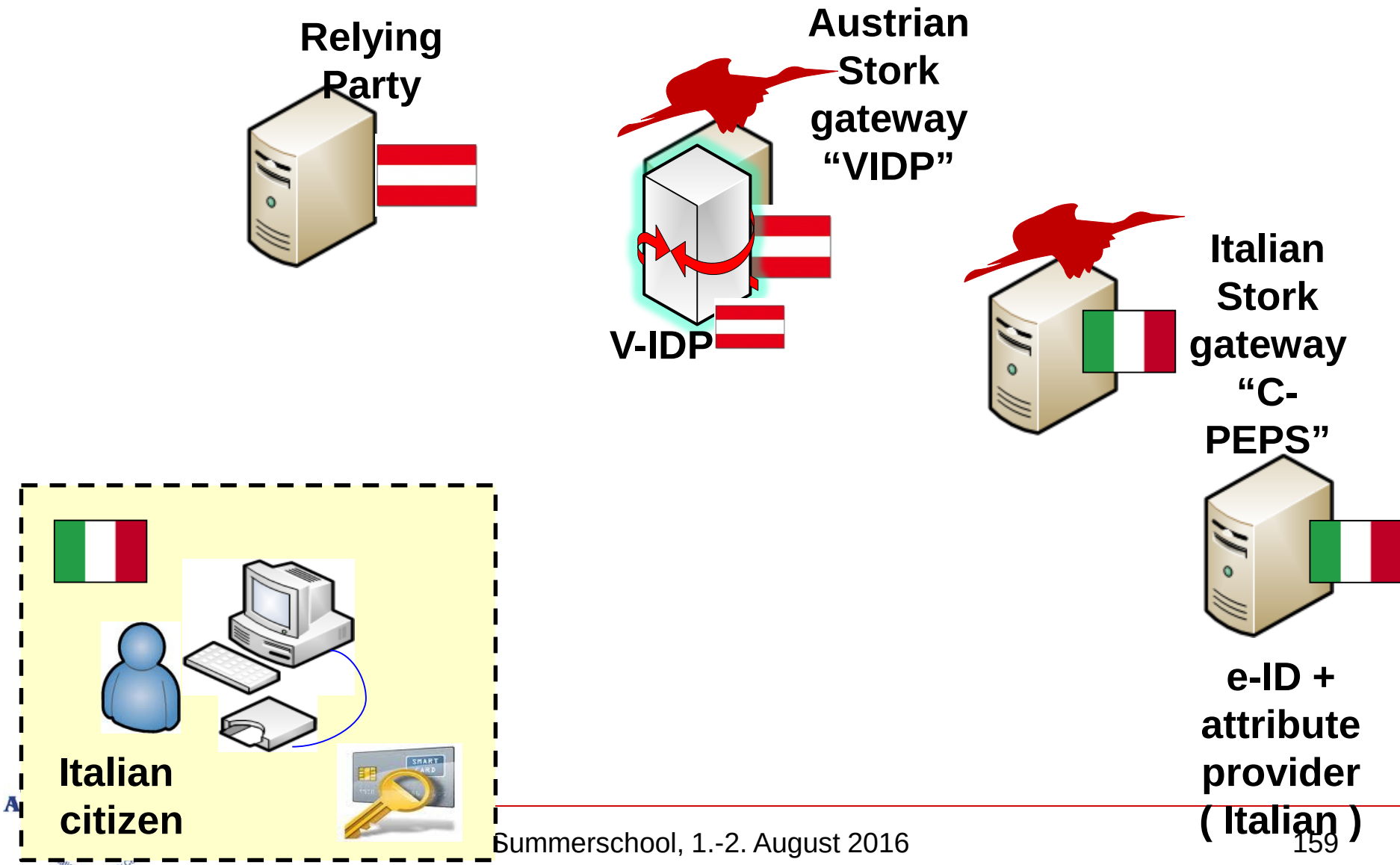
PEPS-VIDP Process

common STORK and MS-specific parts



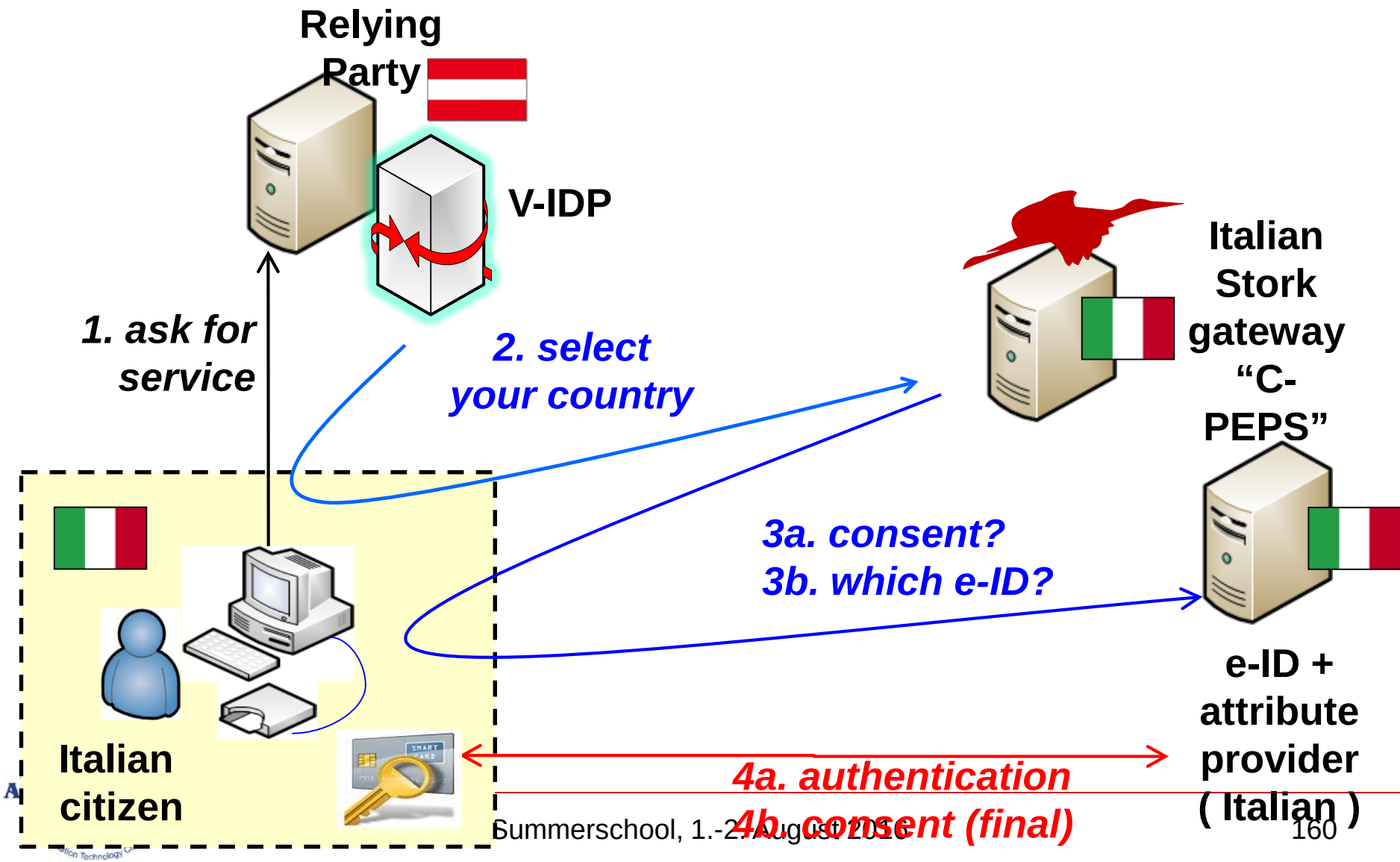
VIDP-PEPS Process

Italian accessing Austrian Relying Party



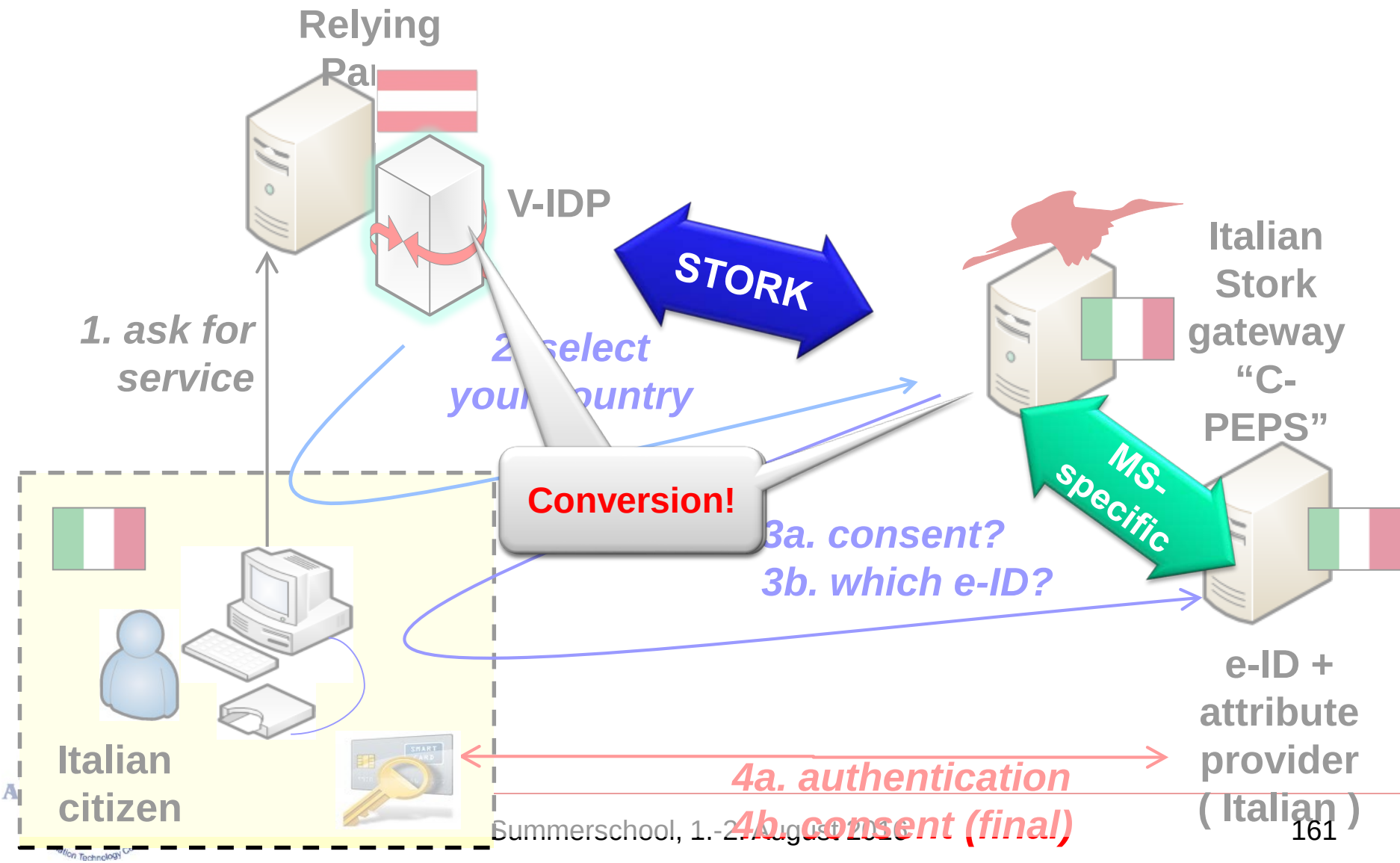
VIDP-PEPS Process

Italian accessing Austrian Relying Party

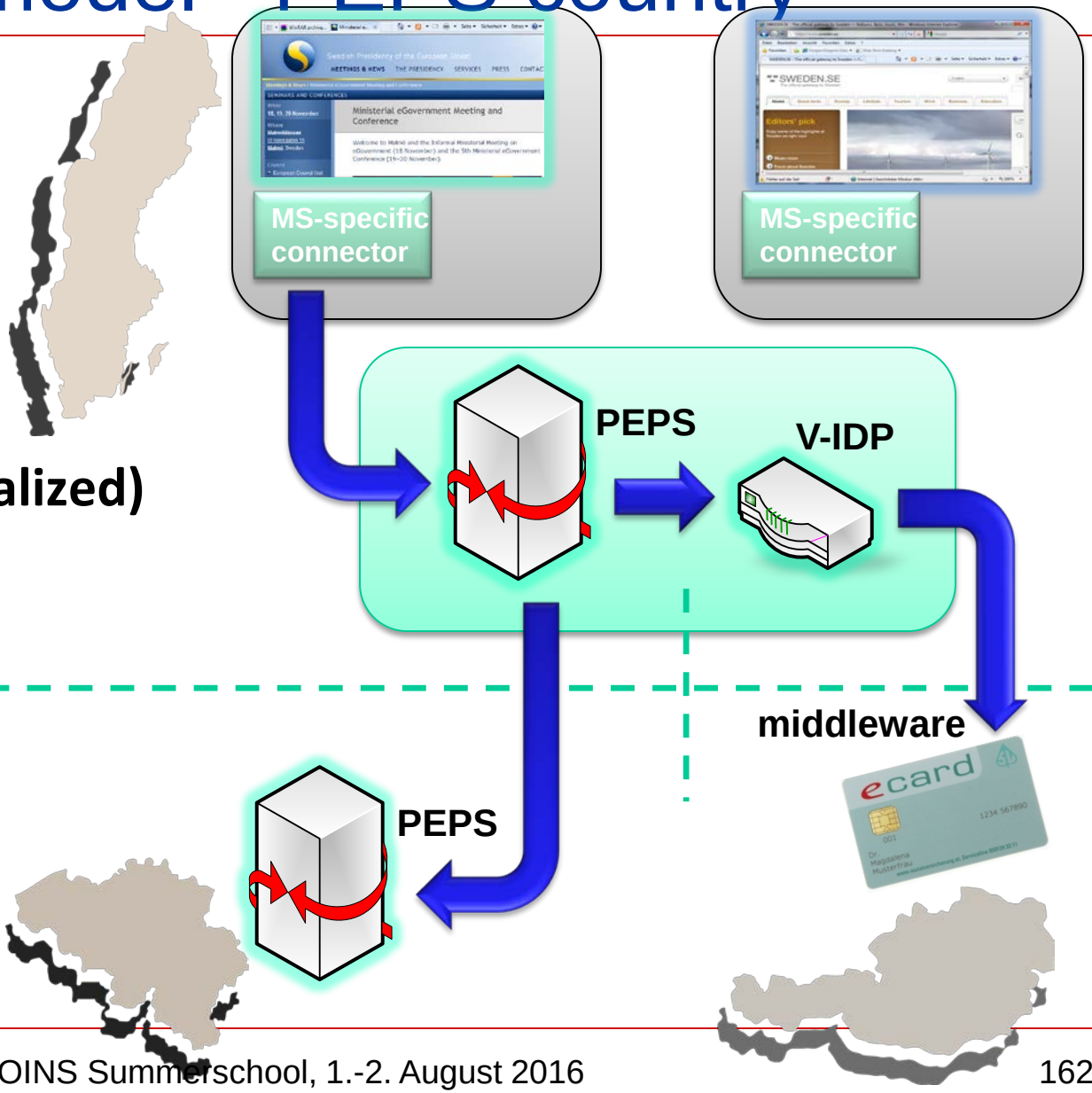


VIDP-PEPS Process

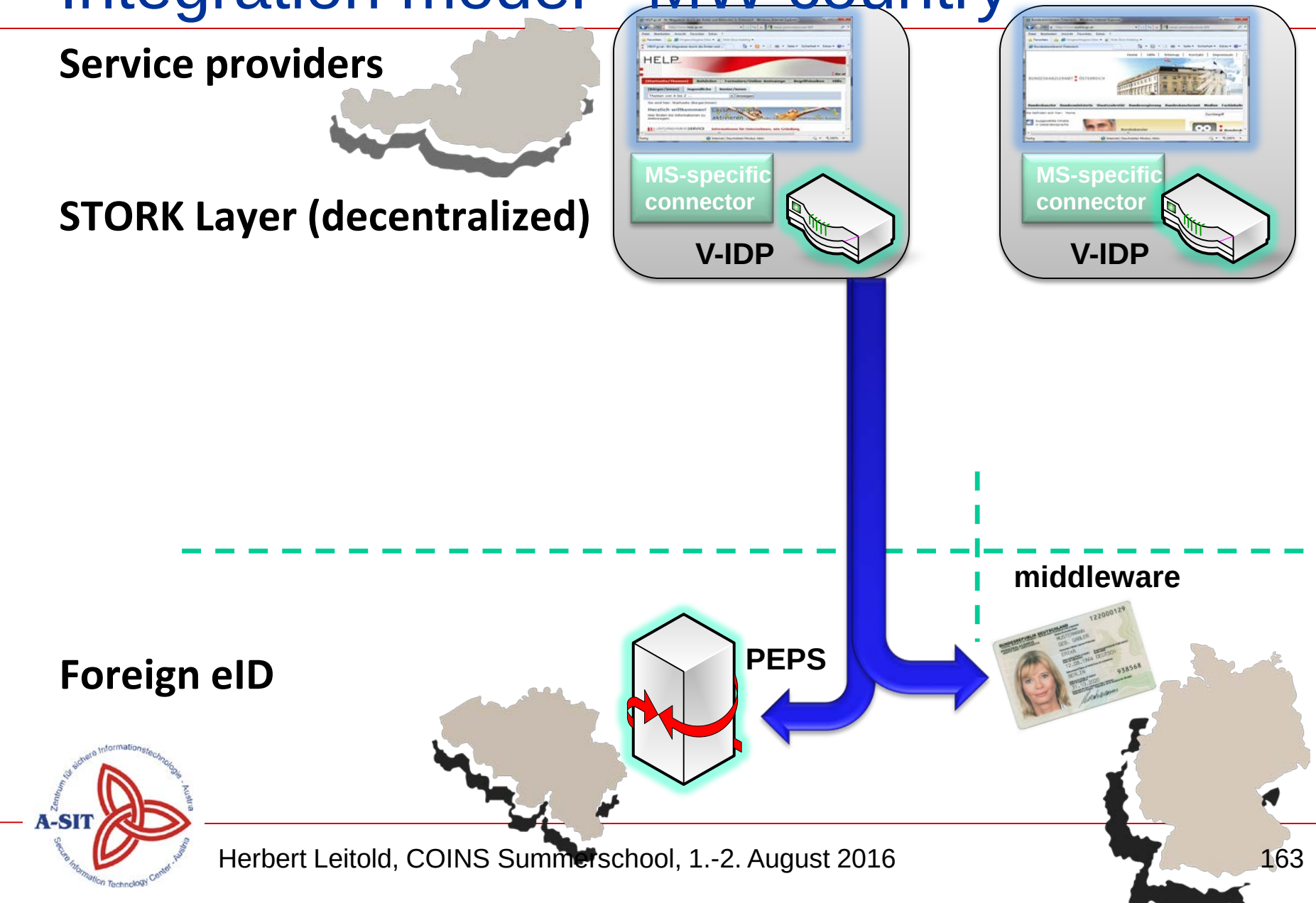
common STORK and MS-specific parts



Integration model "PEPS country"



Integration model "MW country"



STORK making access smarter.eu

SECTION 9: LESSONS LEARNED AND SUSTAINABILITY

General considerations

- Middleware
  - No intermediaries between user & SP
    - SP remains data controller
  - Needs to integrate all tokens (pure model)
  - End-to-end security

- PEPS
  - Third party
    - Liability shift
    - Data processor or data controller
  - Hides national complexity
  - Segmented trust-relationships

In both cases consent as basis for data processing legitimacy

Overview of lessons learned (STORK-1)

- Technical issues are minor
  - e.g. integration with legacy systems
  - e.g. standardization / lacking standards
- Operational issues are **relevant**
  - needs governance
  - needs support and maintenance
  - needs getting the message to IdPs and SPs
- Legal issues are **key**
  - Data Protection
  - Liability
  - Mutual recognition

Data Protection

- Consulted with Art. 29 WP
- Data controller / processor
  - Clear situation in the MW model
  - Art. 29 refers to „dilemma“, as both can be argued
    - *Therefore controllers that use a PEPS and provider of PEPS services will have to decide if they consider themselves as controller or processor under the Directive 95/46 and contact their national DPA to confirm this for example during a notification procedure*
- Data security
  - Art. 29 sees **common minimum standards** desirable
  - Guidelines for SPs on which QAA level to use
    - Art. 29 notes that there is no lack of harmonisation of national frameworks regulating level 4 (qual. cert.)

Liability / Mutual recognition

- No mission-critical services without clear responsibilities and liability
- No take-up without mutual recognition

Liability, Legal (Un-)Certainty

- Where we actually “got stuck”
  - We integrated with ECAS - a major success
  - The STORK and ECAS ambition has been higher:
    - In 2010 National Emission Trading Registries in the had serious fraud
    - The EC Registry that launched end of 2011 integrates with ECAS
    - Technical integration with STORK high-security would have been easy
    - We could not integrate STORK due to **legal uncertainty** & **unclear liability**

SPIEGEL ONLINE INTERNATIONAL

Climate Crime

Phishing Scam Cripples European Emissions Trading

Trading in CO2 emissions allowances has been hampered in several European countries as a result of a phishing scam. AP

Sneaky cyber-thieves have made millions by fraudulently obtaining European greenhouse gas emissions allowances and reselling them. The scam has hampered trading of the credits, which are seen as an important tool in curbing climate change in several European countries.

Most Internet users are familiar with the e-mail scam known in the

Sustainability

Interoperability Solutions for European Public Administrations

- Became part of the ISA Work Programme
- ISA Action 1. “STORK Sustainability”
  - Budget: 1.350 k€

- Two main action items
  1. Governance activities
  2. Development works

… to have it maintained

- Maintenance, update and upgrade of the Common SW modules:
  - Implement agreed changed in the common software, as well for PEPS as for V-IDP
  - Test changes in all relevant environments (Tomcat, JBoss, Glassfish; all on Windows / Linux) and others according to MS needs
  - Test compatibility with actual production versions
  - Maintenance of test-laboratory
  - Publish the new software, together with release notes
  - Active bug-tracking and error solution
  - Technical support for the Member States 8x5x52

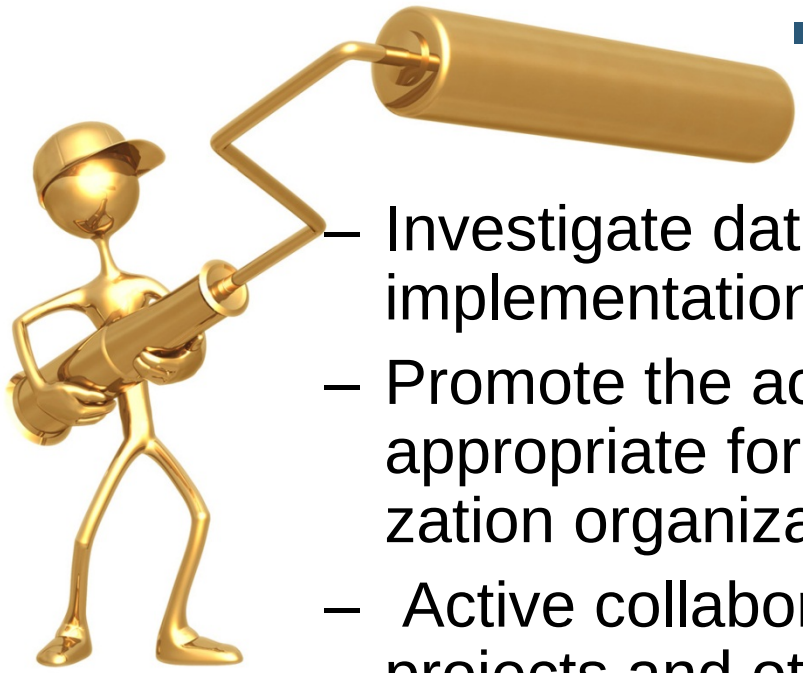
To get grip on governance (I/II)

- Update of Common Specifications (CS):
  - Initiate and coordinate discussions on new data or data to be changed as well as new functionalities or actual ones to be changed.
  - Reflect agreed changes in documentation.
  - Quality control on the implementation of changed specifications
  - Coordinate support groups.
  - Coordinate implementation in Member States.
  - Quality assessment for implementation with new/ changed Service Providers and new Member States.
  - etc.

To get grip on governance (II/II)

- Update of the QAA levels according to the following task breakdown:
  - Once a year to discuss, vote on and formally agree on changes.
  - Twice a year collect by e-mail change requests.
  - Twice a year the dissemination of an assessment of requested changes.
  - Once a year a publication of an updated "QAA" document.

To get it taken up



- Standardization as a basis of industry take-up
  - Investigate data standards and promote their implementation.
  - Promote the acceptance of the CS in appropriate forums (eGOV events, standardi-zation organizations, Industry players…).
  - Active collaboration with EU sponsored projects and other sectoral eGOV solutions across-Europe;
  - propose changes to the common specs which are required or useful to those projects.

SECTION 10: STORK 2.0

Why STORK 2.0?

WHY STORK 2.0?

ANYTHING MISSING?

What hasn‘t been achieved so far …

- Representation and mandates; attribute provision
  - STORK 1 limited to natural persons on their own behalf
  - Limited to the basic person attributes (name, DoB, …)
- High attack potentials or access to sensitive data
  - Security addressed, but STORK 1 pilots no valuable targets
- Private sector services and service providers
  - STORK 1 was eGov services. Not by design, but in fact
- Liability and recognition
  - STORK 1 had no provisions, if something “goes wrong”
- Standardization and business models
  - STORK 1 did specifications, but no standards

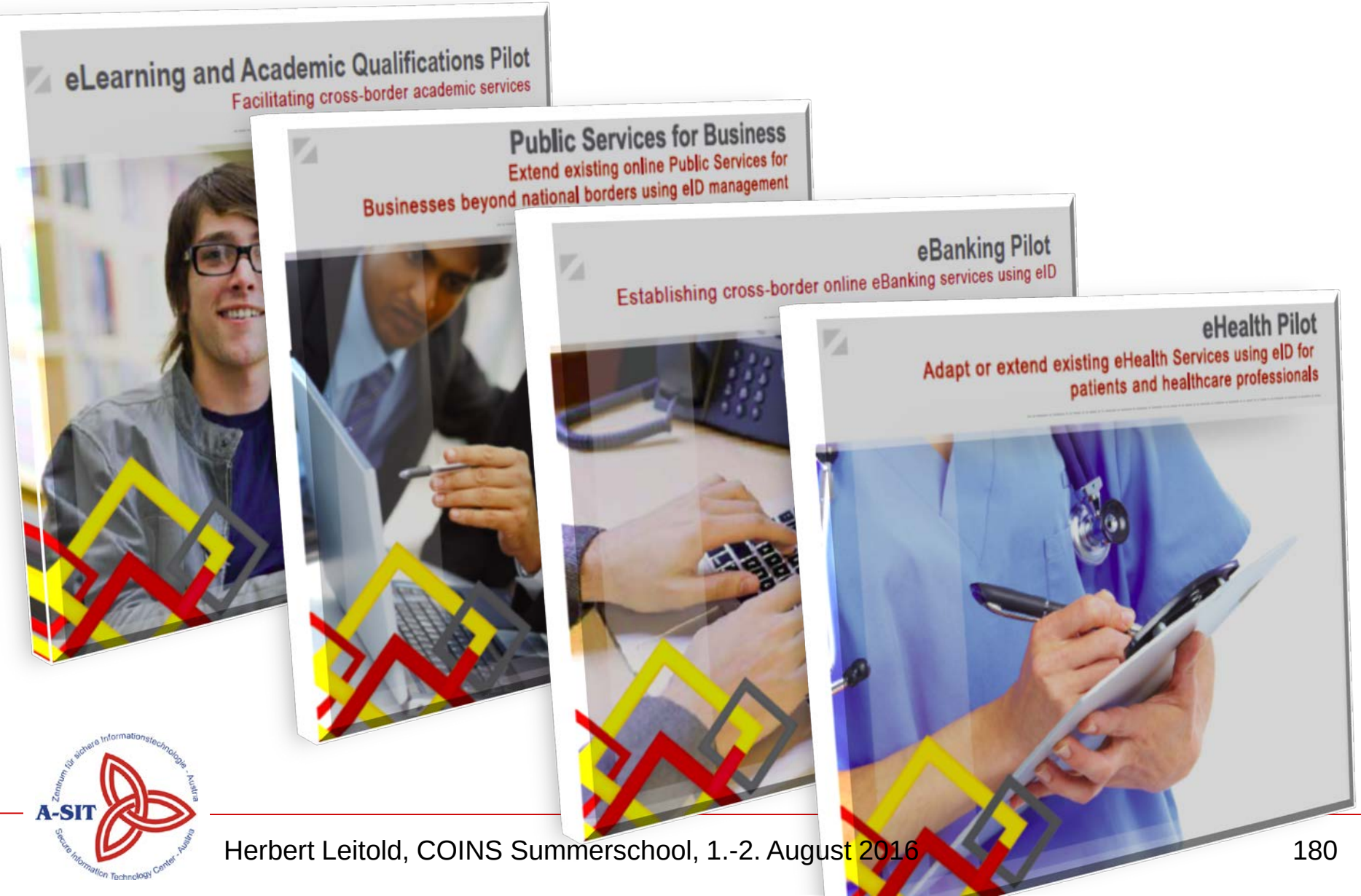
… is addressed by

- Representation and mandates; attribute provision
  - **Core of STORK 2.0 common specifications and all pilots**
  - **Representation of a legal person; mandate of another**
- High attack potentials or access to sensitive data
  - **STORK 2.0 eHealth and Internet banking pilot**
- Private sector service providers
  - **Company services and Internet banking pilot**
- Liability and recognition
  - **eIDAS Regulation!**
- Standardization and business models
  - **EC ISA, CEF and dedicated WP on eID service offerings**

New function: Attribute provision

- Legal person identification
  - "*Authentication*" => "*Authentication on behalf*"
  - Derives mandates from authoritative source
    - E.g. query Business Registers for legal representative
  - Assigns attribute quality assurance (AQAA)
- Domain-specific attributes
  - e.g. in eHealth to identify health care providers
  - e.g. in eAcademia "*isStudent*", "*hasDegree*", …

The STORK 2.0 Pilots



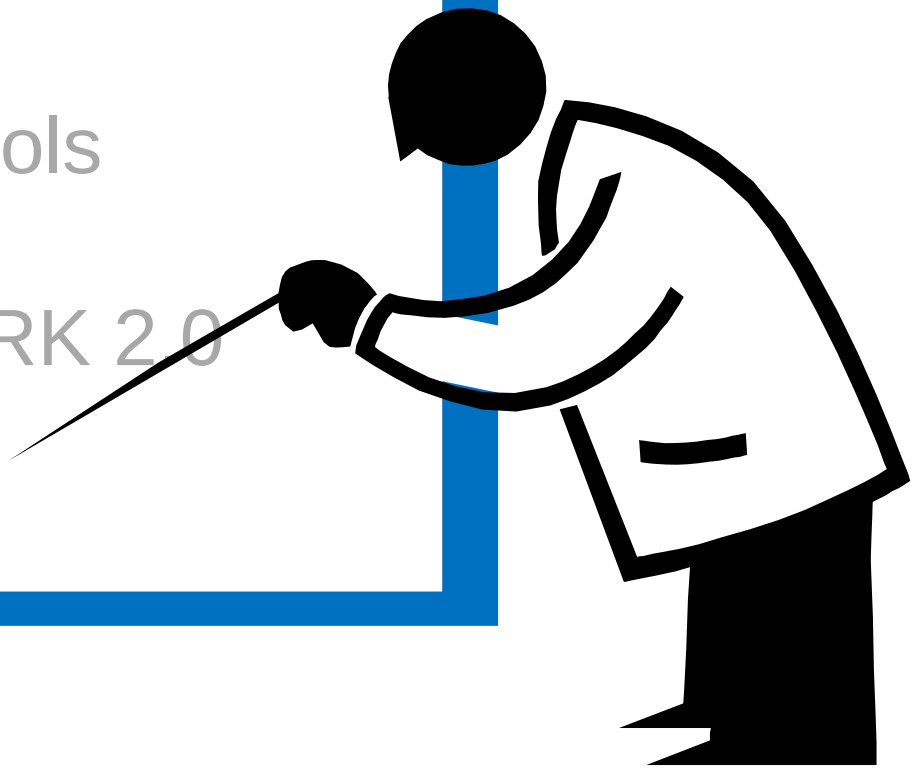
Demos

- Authenticate at European Commission Services

- Authenticate as legal representative of a company

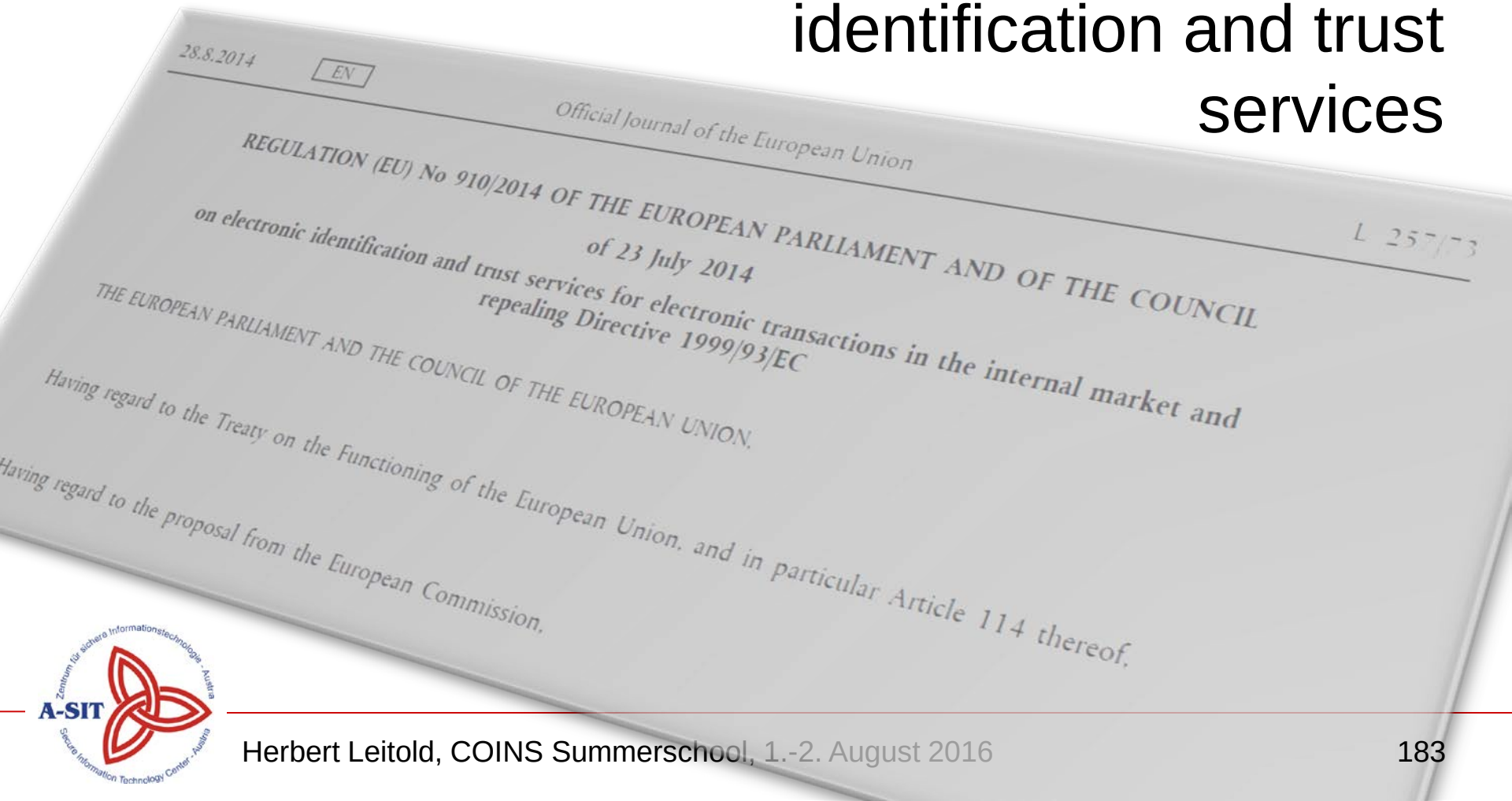
Contents

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



Recent policy development

- eIDAS: Regulation on electronic identification and trust services


28.8.2014 EN

Official Journal of the European Union

L 257/73

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

SECTION 11: EIDAS GENERAL

Signature Directive vs. eIDAS Regulation

- The Signature Directive was enacted in 1999
  - Transposed to national laws (Austrian Signature Act)
- The eIDAS Regulation was enacted in July 2014
  - A Regulation applies directly (no national laws)
- Covers “eID” and “trust services” / “trust service providers”
  - mutual recognition of *notified* eID
  - electronic signatures
  - electronic seals
  - eDocument admissibility
  - Website authentication
  - electronic delivery

Two main parts of eIDAS

- eID
  - Notification, Recognition, Coordination

MS sovereignty, but recognition obligation
(Coordination on interoperability and security)

- Trust services
  - electronic signatures
  - electronic seals
  - validation, preservation
  - electronic timestamps
  - el. registered delivery
  - website authentication

Harmonisation (Supervision, Liability, Recognition, Formats, Trust Lists, …)

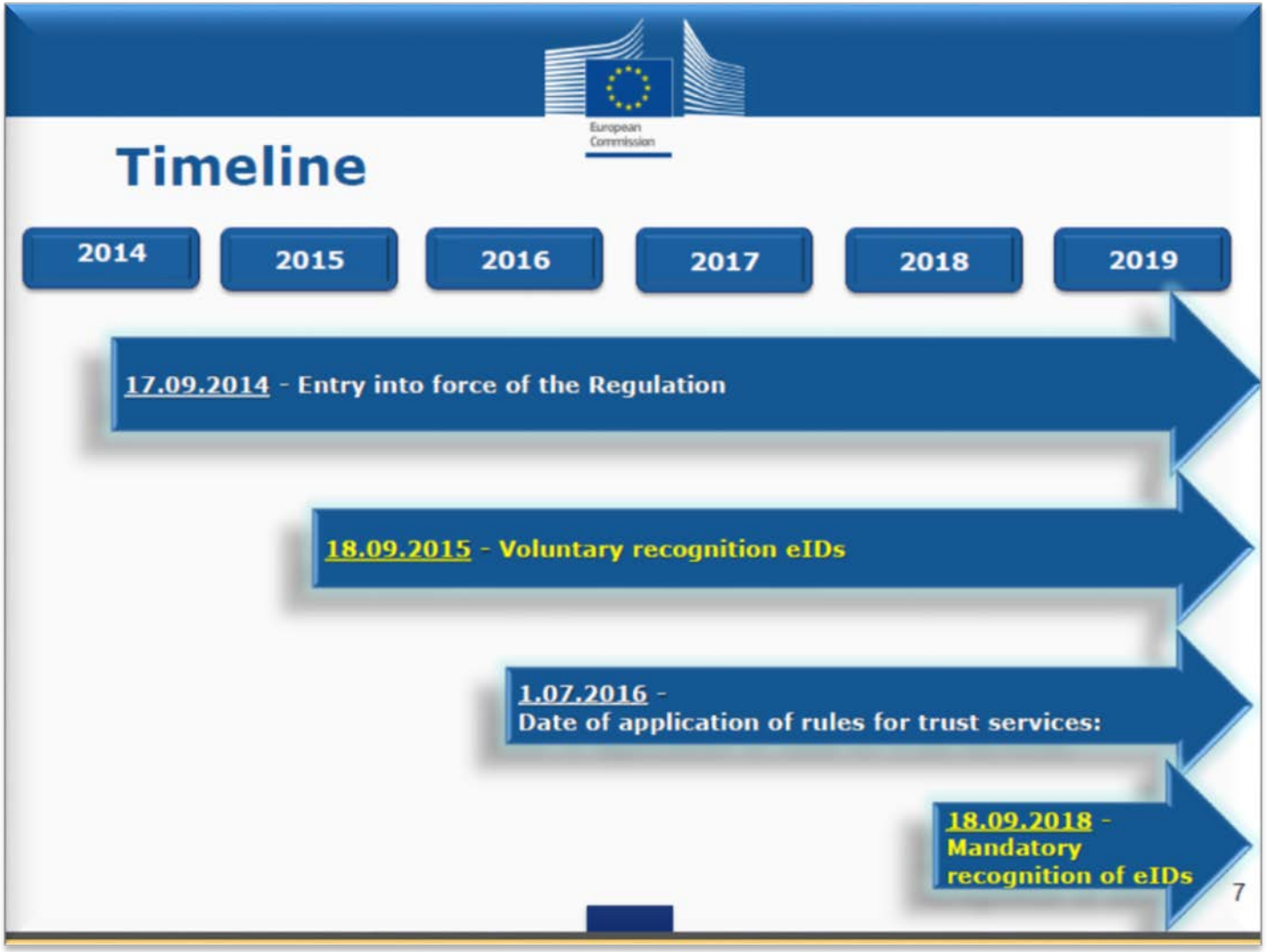
eIDAS Trust Services

Horizontal principles: Liability; Supervision; International aspects; Security requirements; data protection; Qualified services; Prior authorisation; trusted lists; EU trust mark

- Electronic signatures ,including validation and preservation services
- Electronic seals, including validation and preservation services
- Time stamping
- Electronic registered delivery service
- Website authentication

Source: Andrea Servida (European Commission), Mobile eID Forum, 29 April 2015

eIDAS eID Timeline



Source: Andrea Servida (European Commission), Mobile eID Forum, 29 April 2015

eID Key Principles

- Based on “notified eID”
  - Member State decides, if/what eID scheme to notify
  - 3 Levels of Assurance (LoA) “high”, “substantial”, “low”
- Recognition of notified eID
  - Mandatory for public services LoA “high” & “substantial”
  - Voluntary for private services
- Interoperability and cooperation of MS
  - Based on STORK
- Implementing acts on …
  - LoA, Interoperability Framework, Cooperation, …

eIDAS quotes relevant to STORK

- Recital 16:
  Assurance levels should characterise the degree of confidence in electronic identification means […].
  In particular, the Large Scale Pilot STORK and ISO 29115 refer, inter alia, to levels 2, 3 and 4, which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurances levels low, substantial and high within the meaning of this Regulation […]
- Definition of eID:
  '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 who represents a legal person;

eIDAS: Recognition

- Mutual recognition (12 month after publ. of the list)
  […] *the electronic identification means issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that service online, provided that the following conditions are met:*
  - *(a) the electronic identification means is issued under an electronic identification scheme that is included in the list published by the Commission pursuant to Article 9;*
  - *(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;*
  - *(c) the relevant public sector body uses the assurance level substantial or high in relation to accessing that service online.*

eIDAS: Authentication means

- Art. 7 (f)
  the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State can confirm the person identification data received in electronic form.
  For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication.
  The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body.
  Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements prevent or significantly impede the interoperability of the notified electronic identification schemes;

eIDAS: LoA impelementing act

- Art. 8 (3)
  By taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means for the purposes of paragraph 1.
  Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of:
  (a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;
  (b) the procedure for the issuance of the requested electronic identification means;
  (c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;
  (d) the entity issuing the electronic identification means;
  (e) any other body involved in the application for the issuance of the electronic identification means; and(f) the technical and security specifications of the issued electronic identification means.

Cooperation means

- Art. 12
  1. The national electronic identification schemes notified in accordance with Article 9 shall be interoperable.
  2. For the purposes of paragraph 1, the interoperability framework shall be established.
  3. The interoperability framework shall meet the following criteria:
     …
  4. The interoperability framework shall consist of:
     …
  5. Member States shall cooperate with regard to the following:
     (a) the interoperability of the electronic identification schemes notified pursuant to Article 9(1) and the electronic identification schemes which Member States intend to notify; and
     (b) the security of the electronic identification schemes.
     …
  6. The cooperation between Member States shall consist of :
     …

eIDAS eID Notification Process

1. MS pre-notification
   - MS describe eID scheme(s) and their LoA
   - Show how LoA requirements are met
2. Peer Review
   - Other MS assess the eID scheme(s)
   - Cooperation Network opinion (non-binding)
3. MS Notification

4. Publication by EC

Minimum 6 months

Max. 2 months

On Recognitions

- All MS have to recognise all notified eIDs at LoA substantial or high in all public services
  - If the service is eID enabled
  - even if the MS does not notify its own eID
- MS voluntarily can accept LoA low
- Authentication is free of charge for public services
- Private sector use is encouraged, but no obligation
- Notifying MS may set conditions for private sector use

SECTION 12: EIDAS EID IMPLEMENTATION

eIDAS: Main differences to STORK (I/II)

- QAA redefined to LoA
  - Outcome based approach
- Components redesigned
  - PEPS and VIDP become “eIDAS nodes”
    - An “eIDAS Service” authenticates citizens
      - Can still be proxy or middleware (deployed at receiving MS)
    - An “eIDAS Connector” interfaces to Relying Parties
      - Can be several per MS in any case (e.g. sectorial)

eIDAS: Main differences to STORK (II/II)

- Technical specifications revised
  - Closer to current standards
    - Aligned with Kanatra eGov profile where possible
    - Attributes follow ISA Core Vocabulary
  - Assertion encryption
    - At the cross-border interfaces (MS may nationally)
  - Uses SAML Metadata
  - Included specifics that came with eIDAS
    - E.g. distinction between public and private sector

Levels of Assurance LoA

- MS assign eID schema LoA *low*, *substantial*, *high*
- LoA is defined in Implementing Act 2015/1502
  - Took STORK and ISO 29115 into consideration, but followed an outcome-based approach
- Distinguished through quality of:
  - Enrolment
  - eID Means management
  - Authentication
  - Management and Organisation

LoA – Enrolment

- Application and registration
  - e.g. that applicant is aware of terms
- Identity proofing and verification
  - For *substantial* or *high* e.g. verifying the possession of a photo ID, or linking to previous identification (plus some further variants / measures)
- Binding between the electronic identification means of natural and legal persons

LoA – eID Means management

- eID means characteristics
  - e.g. for *substantial* / *high* multi-factor autentic.
  - for *high* also tamper proof and designed so it can be reliably protected against use by others
- Issuance, delivery and activation
  - for *high* delivery into possession of applicant
- and requirements for suspension, revocation, reactivation, renewal and replacement

LoA – Authentication

- Authentication mechanism
  - at all levels protect stored data against loss and against compromise, including analysis offline
  - at *substantial* or *high* dynamic authentication
  - at *high* also protect against guessing, eaves-dropping, replay or manipulation of communi-cation by an attacker with <u>high attack potential</u>

LoA – Management and Organisation

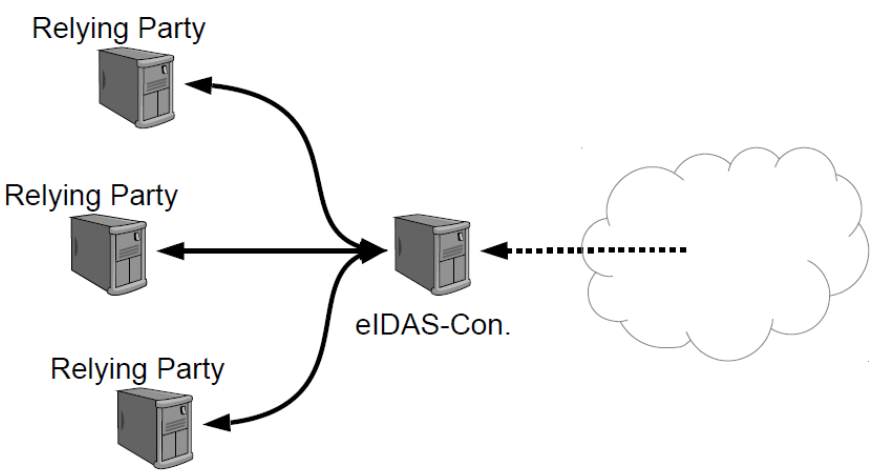
- Ensure that documented information security management practices, policies, approaches to risk management, and other recognised controls are in place
- Requirements on record keeping, facilities, staff, technical controls, etc.
- Most of these managerial and organisational requirements equally apply to all LoA levels

eIDAS Technical Specifications

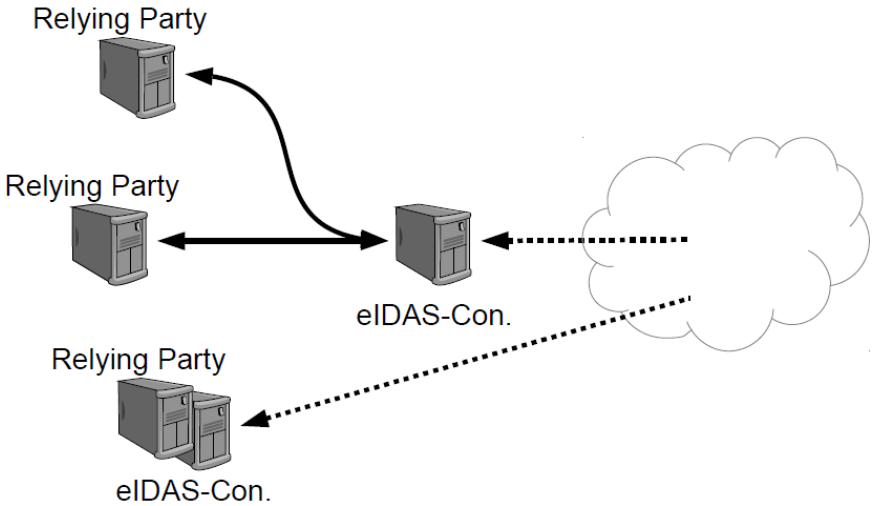
1. Interoperability Architecture
   - Overview, General Requirements
2. Message Format
   - SAML 2.0 Profile
3. Attribute Profile
   - Minimum Data Set based on ISA Core Vocabulary
4. Crypto Requirements
   - Crypto Suites for TLS and SAML

ad “1. Interoperability Architecture”

- Options at receiving MS



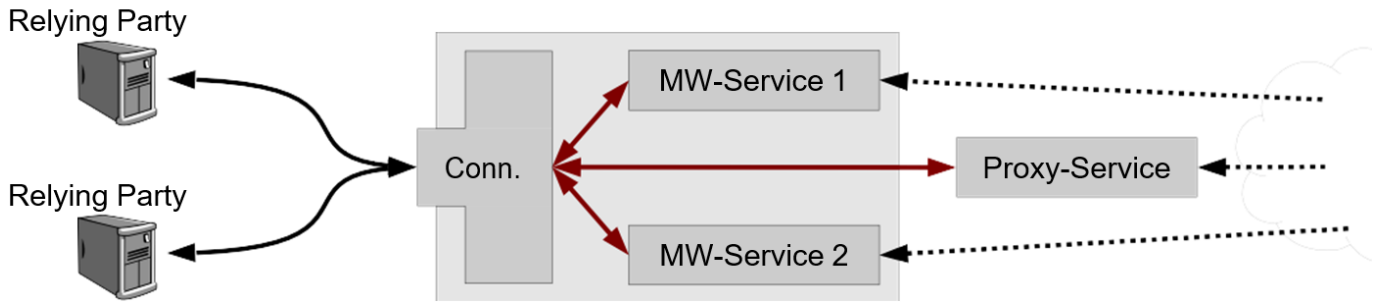
Centralized MS



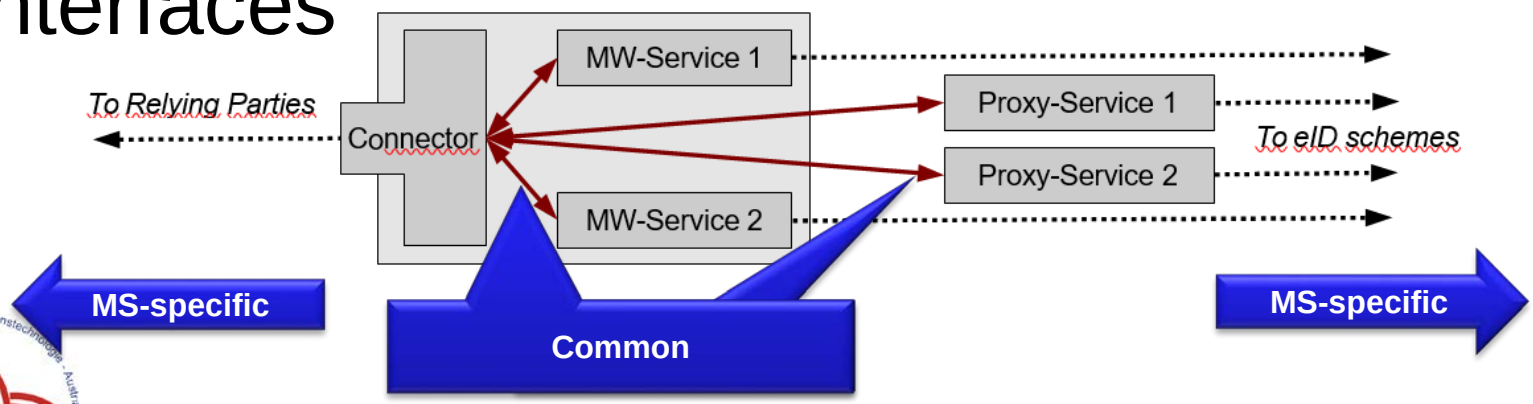
Decentralized MS

ad “1. Interoperability Architecture”

- Receiving MS components

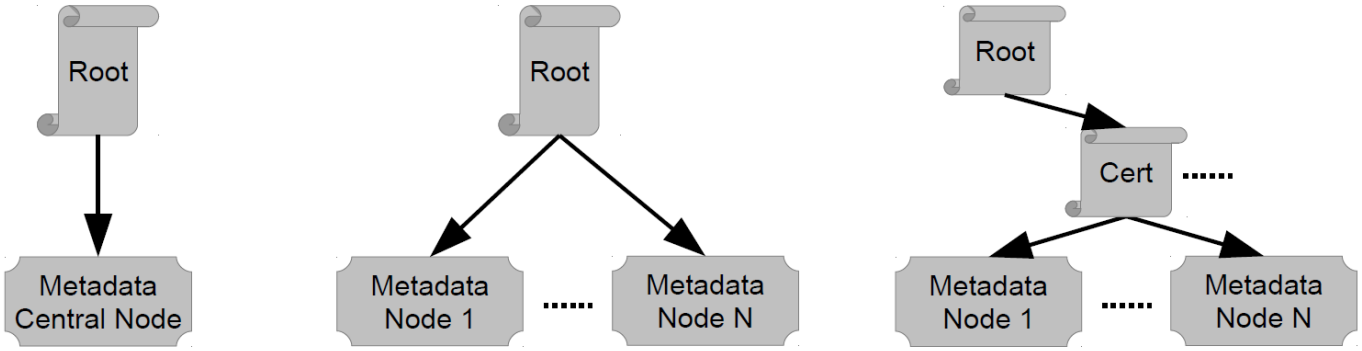


- Interfaces



ad “1. Interoperability Architecture”

- eIDAS SAML Metadata Trust model
  - Trust Anchor is a MS root
    - Root can sign nodes’ MD-files directly or delegate



  - Each MS should publish a structures list of metadata-locations for prefetching and caching

ad “1. Interoperability Architecture”

- Interoperability Architecture also specifies
  - Process flow
    - As shown for STORK (Rel. Party → Connector →…)
  - SAML Bindings
    - For Requests HTTP-POST or -REDIRECT *(recomm.)*
    - For Responses HTTP-POST
      - Only if *AssertionConsumerService* listed in SAML Metadata
  - Security requirements
    - e.g. ISO 27001 compliance or similar

ad “2. Message Format”

- SAML 2.0 profile that took into consideration
  - Kantara eGovernment Implementation Profile
  - STORK 2.0 (final common specifications D4.4)
- Specifies
  - Metadata Format
  - SAML AuthnRequest and Response
    - Basic attributes (LoA) and SP type (public/private)
    - MDS-attributes specified in separate document
    - defines extensibility to domain-specific attributes

ad “2. Message Format” | Metadata Example

```
<md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="false"
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <md:KeyDescriptor use="signing">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>MIID==</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:KeyDescriptor use="encryption">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>MIID==</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
    <EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes 256-gcm"/>
  </md:KeyDescriptor>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
  <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</md:NameIDFormat>
  <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://eidas-connector.eu/post"
    isDefault="true"/>
```

Sign requests, not assertions

I will sign using this cert

I want you to encrypt using that cert and to use AES in GCM mode

And deliver only to that URL using HTTP-POST

ad “2. Message Format” | Metadata contd.

```
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://eidas-service.eu/post"/>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="https://eidas-service.eu/redirect"/>
```

POST or –REDIRECT Request to that URL

```
<saml2:Attribute
  FriendlyName="PersonIdentifier"
  Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
</saml2:Attribute>
```

A unique ID, …

```
<saml2:Attribute
  FriendlyName="FamilyName"
  Name=" http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
</saml2:Attribute>
```

the family name, …

```
<saml2:Attribute
  FriendlyName="FirstName"
  Name=" http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
</saml2:Attribute>
```

the first name, ….

```
<saml2:Attribute
  FriendlyName="DateOfBirth"
  Name=" http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
</saml2:Attribute>
</md:IDPSSODescriptor>
```

and the DOB is what I can deliver!

ad “2. Message Format” | AuthnReq. Example

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:AuthnRequest
   Destination="https://eidas-service.eu/post"
   ID="_171ccc6b39b1e8f6e762c2e4ee4ded3a" IssueInstant="2015-04-30T19:25:14.273Z" Version="2.0"
   xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:eidas="http://eidas.europa.eu/saml-
```

```
      <eidas:RequestedAttributes>
         <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
         <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
         <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/CurrentGivenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
         <eidas:RequestedAttribute Name="http://eidas.europa.eu/attributes/naturalperson/DateOfBirth"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri" isRequired="true"/>
      </eidas:RequestedAttributes>
```

Requesting a set of attributes …

```
   <saml2p:RequestedAuthnContext Comparison="minimum">
      <saml2:AuthnContextClassRef xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
         >http://eidas.europa.eu/LoA/high</saml2:AuthnContextClassRef>
   </saml2p:RequestedAuthnContext>
</saml2p:AuthnRequest>
```

… at LoA HIGH.

(actually asking for at least LoA high, but as it is the highest…)

ad “2. Message Format” | AuthnRespone

```
<saml2p:Status>
  <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</saml2p:Status>
<saml2:EncryptedAssertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    Id="encrypted-data-0-1152532362-41467517-23174"
    Type="http://www.w3.org/2001/04/xmlenc#Content">
    <xenc:EncryptionMethod
      Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
```

Well, the assertion (i.e., the interestuing part) is encrypted, so let‘s decrypt and see.

ad “2. Message Format” | received Assertion

```
  <saml2:AuthnContext>
    <saml2:AuthnContextClassRef>http://eidas.europa.eu/LoA/high</saml2:AuthnContextClassRef>
  </saml2:AuthnContext>
</saml2:AuthnStatement>
<saml2:AttributeStatement>
<saml2:Attribute
  FriendlyName="PersonIdentifier"
  Name="http://eidas.europa.eu/attributes/naturalperson/PersonIdentifier"
  NameFormat="urn:oasis:names:tc:saml2:2.0:attrname-format:uri">
  <saml2:AttributeValue xsi:type="eidas: PersonIdentifierType">
    ES/AT/02635542Y
  </saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute
  FriendlyName="FamilyName"
  Name=" http://eidas.europa.eu/attributes/naturalperson/CurrentFamilyName"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue languageID="en-GR" xsi:type="eidas:CurrentFamilyNameType">
    Ωνάσης
  </saml2:AttributeValue>
  <saml2:AttributeValue eidas:Transliterated="true" xsi:type="eidas:CurrentFamilyNameType">
    Onasis
  </saml2:AttributeValue>
```

LoA HIGH

Unique identifier in specified format:
„<source-country> / <destination country> / <identifier>“

Name in original encoding and transliterated

ad “3. Attribute Profile”

Minimum Data Set defined in Implementing Act 2015/1501

For Natural Persons

- Mandatory
  - current first / family name
  - date of birth
  - unique identifier
    - as persistent, as possible
- Optional
  - First / family name at birth
  - place of birth
  - current address

For Legal Person

- Mandatory
  - current legal name
  - unique identifier
    - as persistent, as possible
- Optional
  - current address
  - VAT number
  - tax reference number
  - *EORI number, or some further identifiers defined in EU legislation*

ad “3. Attribute Profile” Example

Attribute (Friendly) Name	eIDAS MDS Attribute	ISA Core Vocab Equivalent	Notes
FamilyName	Current Family Name	cbc:FamilyName	Encoded as xsd:string
FirstName	Current First Names	cvb:GivenName	Encoded as xsd:string
DateOfBirth	Date of Birth	cvb:BirthDate	Encoded as xsd:date
PersonIdentifier	Uniqueness Identifier	cva:Cvidentifier	Encoded as xsd:string

```
  <xsd:complexType name="CurrentFamilyNameType">
    <xsd:annotation>
        <xsd:documentation>
              Current family name of the natural person.
        </xsd:documentation>
    </xsd:annotation>
    <xsd:simpleContent>
        <xsd:extension base="xsd:string">
            <xsd:attribute ref="LatinScript"/>
        </xsd:extension>
    </xsd:simpleContent>
</xsd:complexType>
```

ad “4. Crypto Requirements”

- For TLS
  - cipher suites that provide perfect forward secrecy
  - Recomm: ECDHE / DHE, ECDSA / RSA; AES_GCM
  - Ell. curves min. 224 Bit, DH min. 2048 Bit
  - EV certificates until 2017, from 2018 qualified certif.
  - Further recomm. like no compression or heartbeat ext.
- For SAML
  - For signatures, key agreement, or key transport EC min. 256 Bit; RSA min. 3072 Bit
  - AES for content encryption

CEF eID Building Block

- Reference implementation provided by the European Commission
  - As an offering to MS
  - Based on STORK
  - Open Source

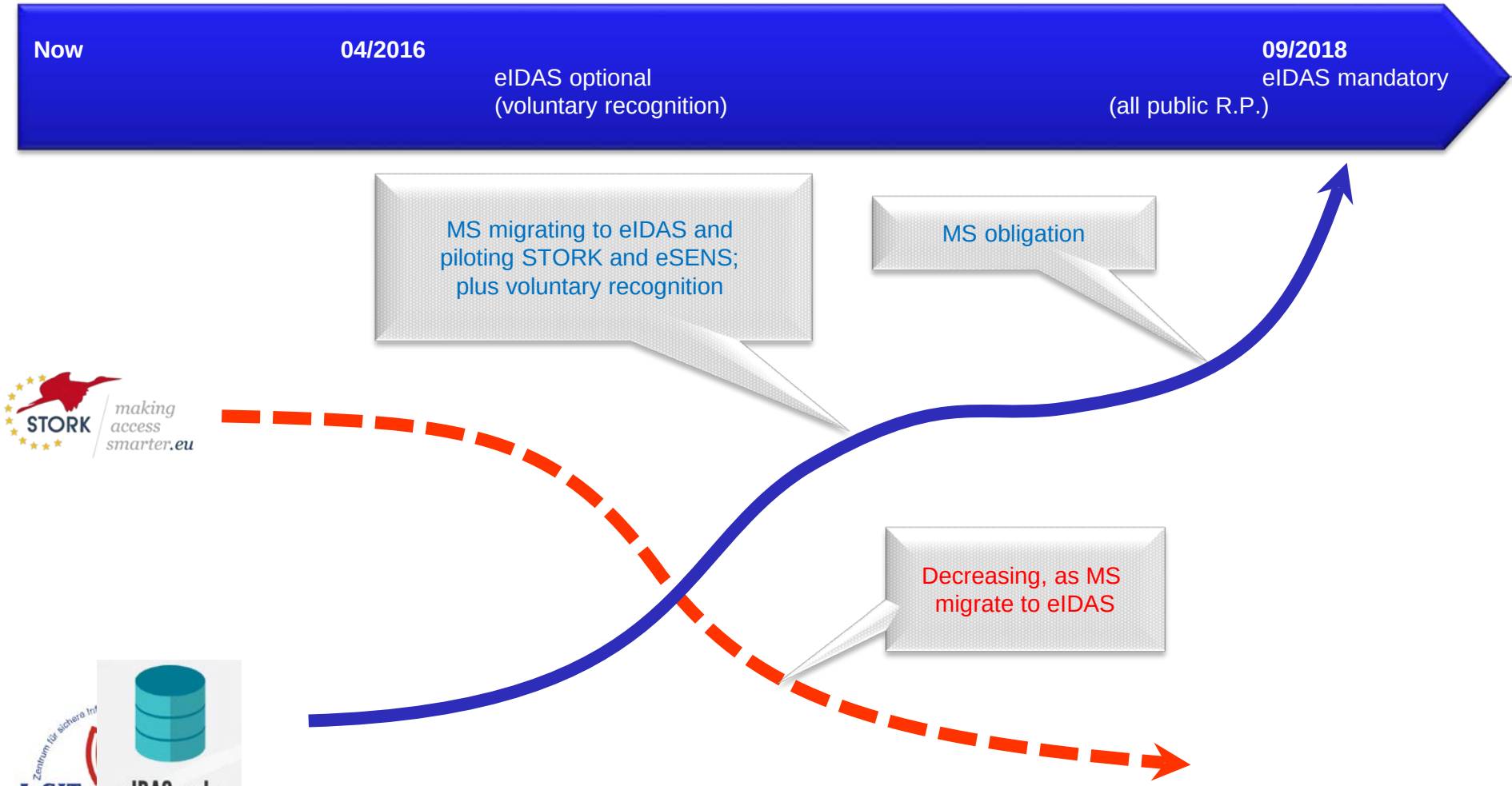
https://ec.europa.eu/cefdigital

eID Building Block versions

- **STORK / STORK 2.0**
  - Current MS infrastructure
  - Production pilots
  - PEPS / VIDP available
- **eIDAS node**
  - MS infrastructure by 09/2018 (at the latest)
  - All public services
  - CEF eID BB v1.0

Protocols are not compatible

Expected infrastructure evolution



How are Service Providers affected?

Now

04/2016
eIDAS optional
(voluntary recognition)

09/2018
eIDAS mandatory
(all public R.P.)

A gap to bridge so MS can seamlessly continue piloting

STORK making access smarter.eu

eIDAS node

A-SIT

Solution to bridge that gap

- Relying party integration shall be able to continue seamlessly
  - Existing STORK pilots, upcoming eSENS pilot, (future RPs)
  - Either using a STORK, eIDAS, or national interface
- STORK eIDAS adaptors as part of the infrastructure
  - Decoupling each MS from other MSs' migration plans
  - Bridging both combinations
    - STORK IdP MS=> eIDAS relying party MS
    - eIDAS relying party MS A => STORK IdP MS
- eSENS implements such an adaptor

Time is flying …

… and my presentation time ends.

Thank you for your patience and attention!