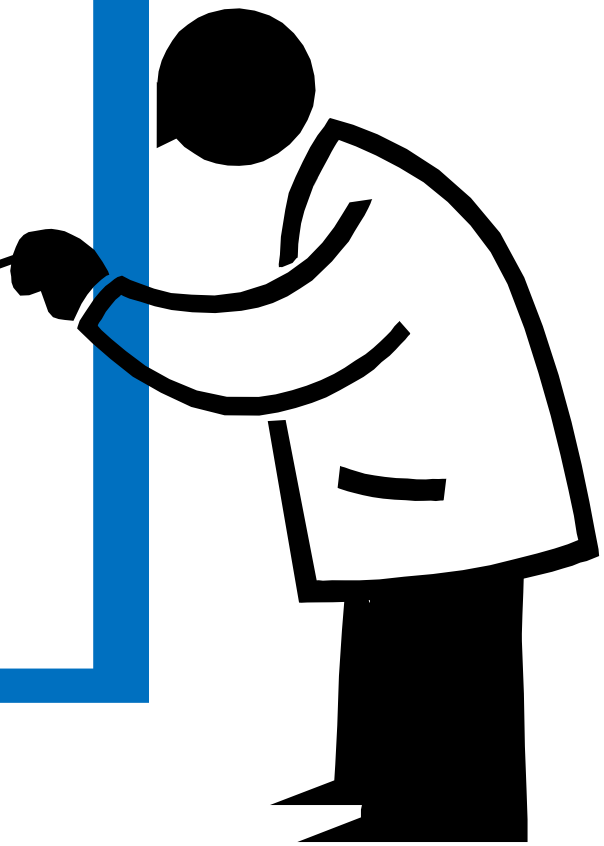
Contents

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



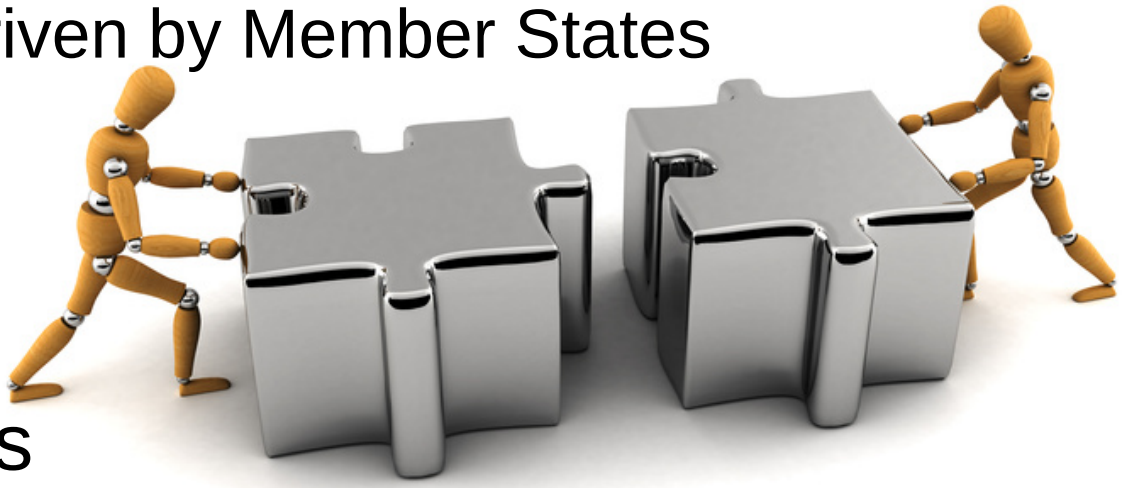
Single Digital Market?

- 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

eCODEX making justice faster.eu

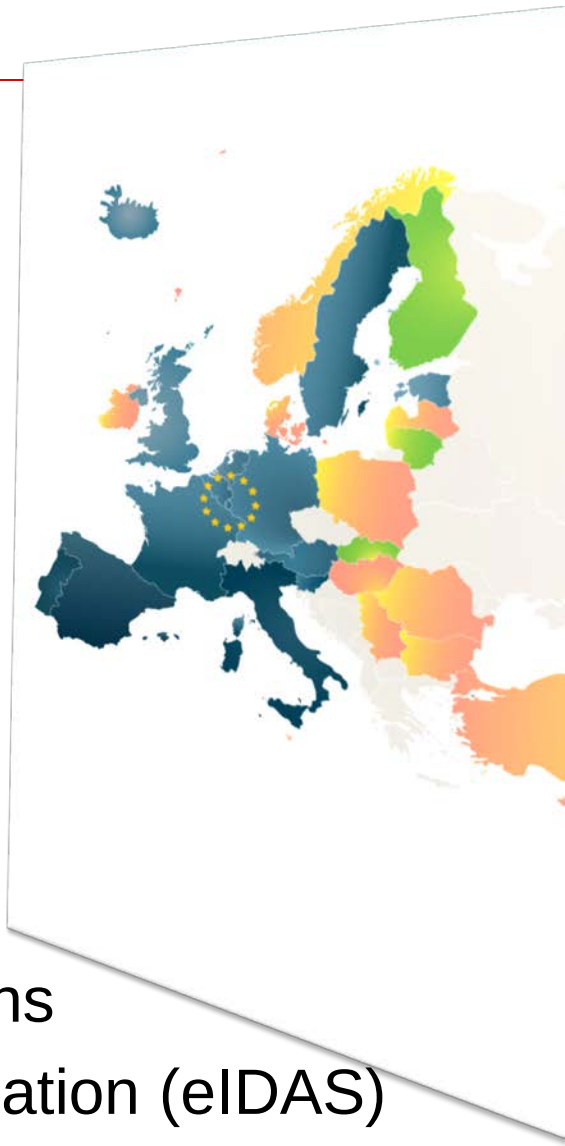
SPOCS making business easier.eu

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

A-SIT Zentrum für sichere Informationstechnologie - Austria Secure Information Technology Center - Austria

SECTION 7: STORK OVERVIEW

STORK Phase 1 Key-facts



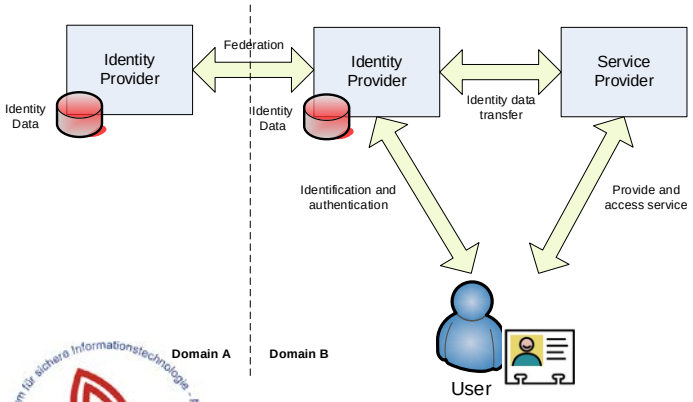
- Project than ran from 2008-2011
- National eID federation between
  - 18 MS
  - 100+ national eID token types
  - 6 pilots in production systems
- Resulted in
  - Open specifications (SAML 2 + QAA)
  - Open source reference implementations
  - Lessons learned as basis for EU legislation (eIDAS)

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

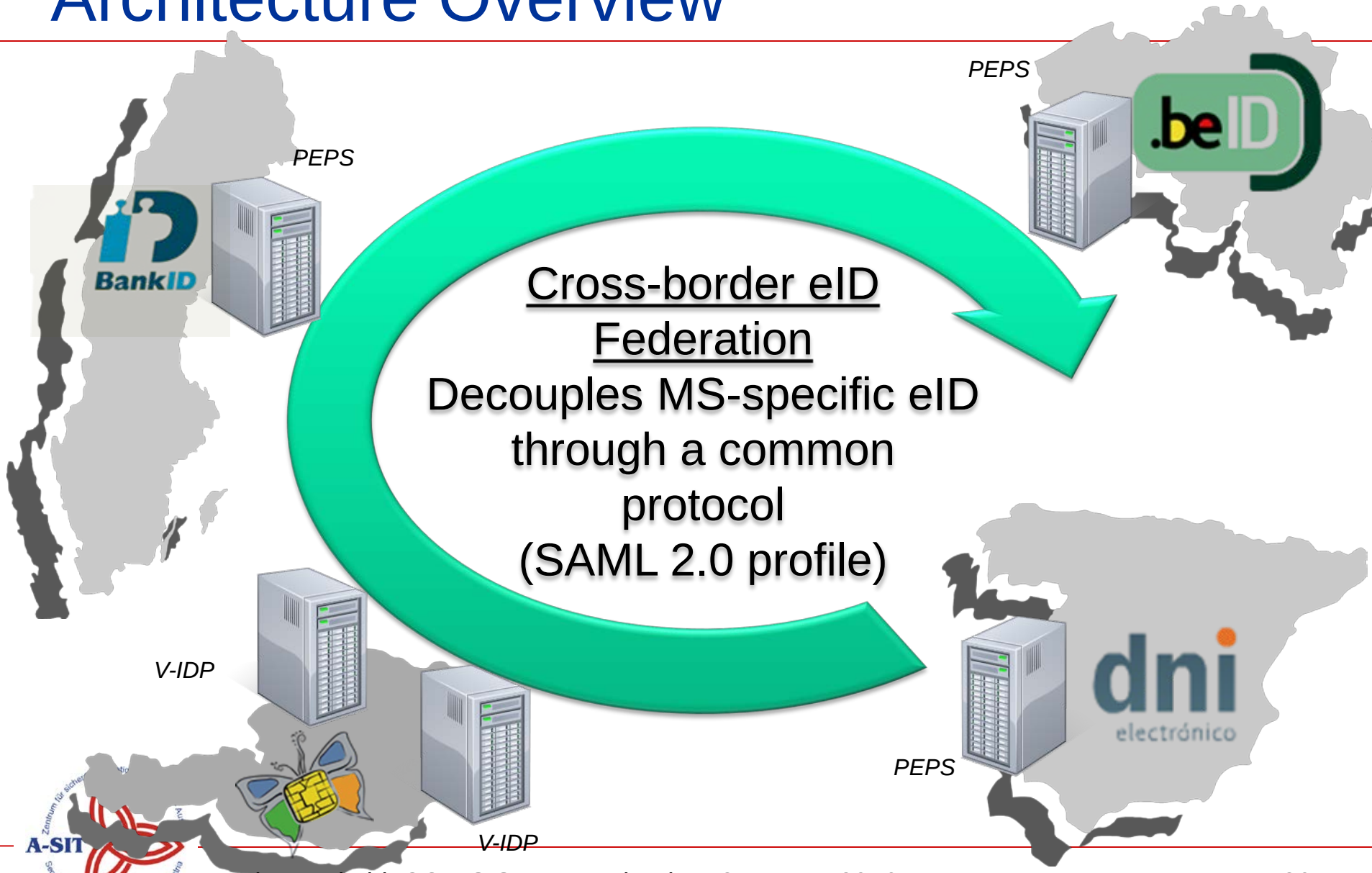
Overall principle

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

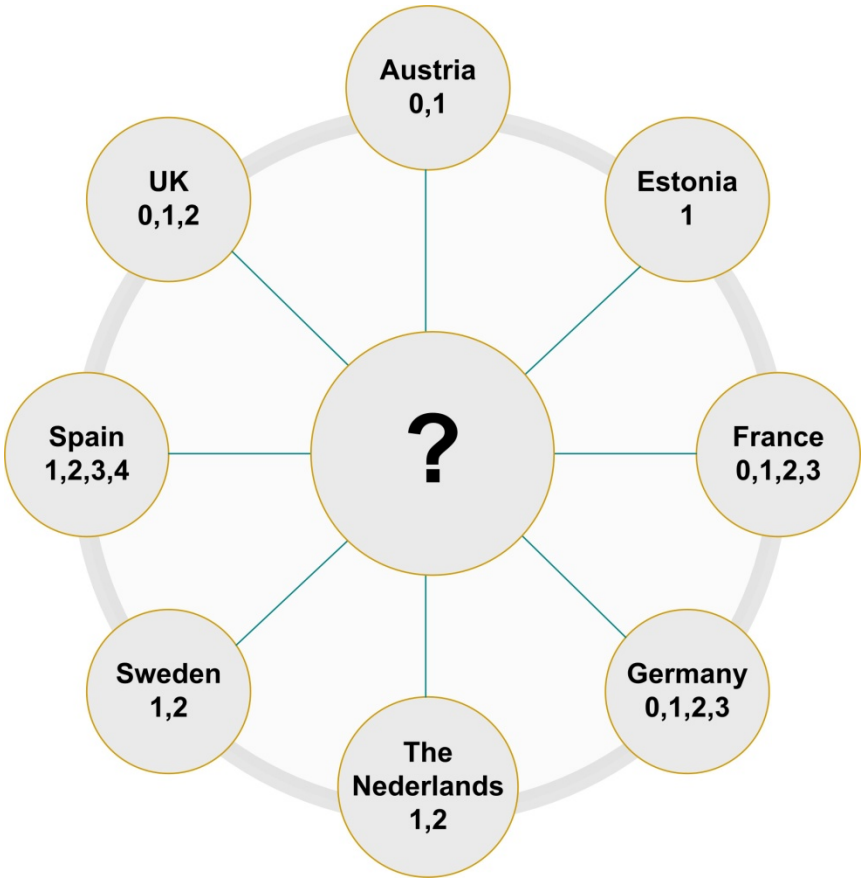


The pilots

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

Affiliate

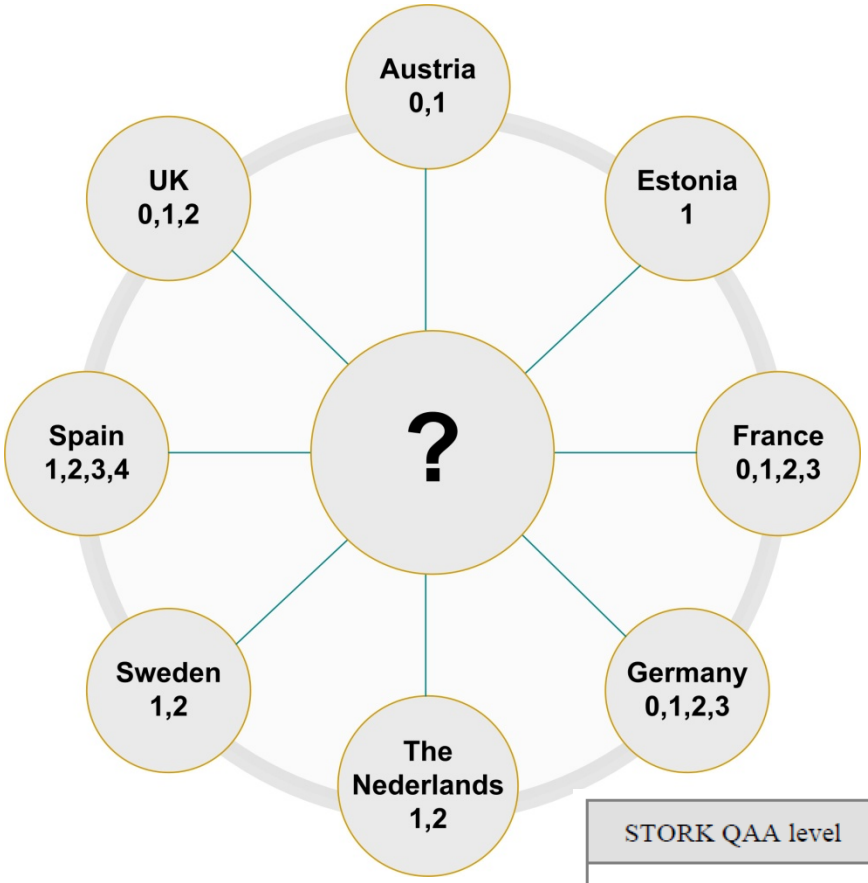
One problem tackled: Trust levels

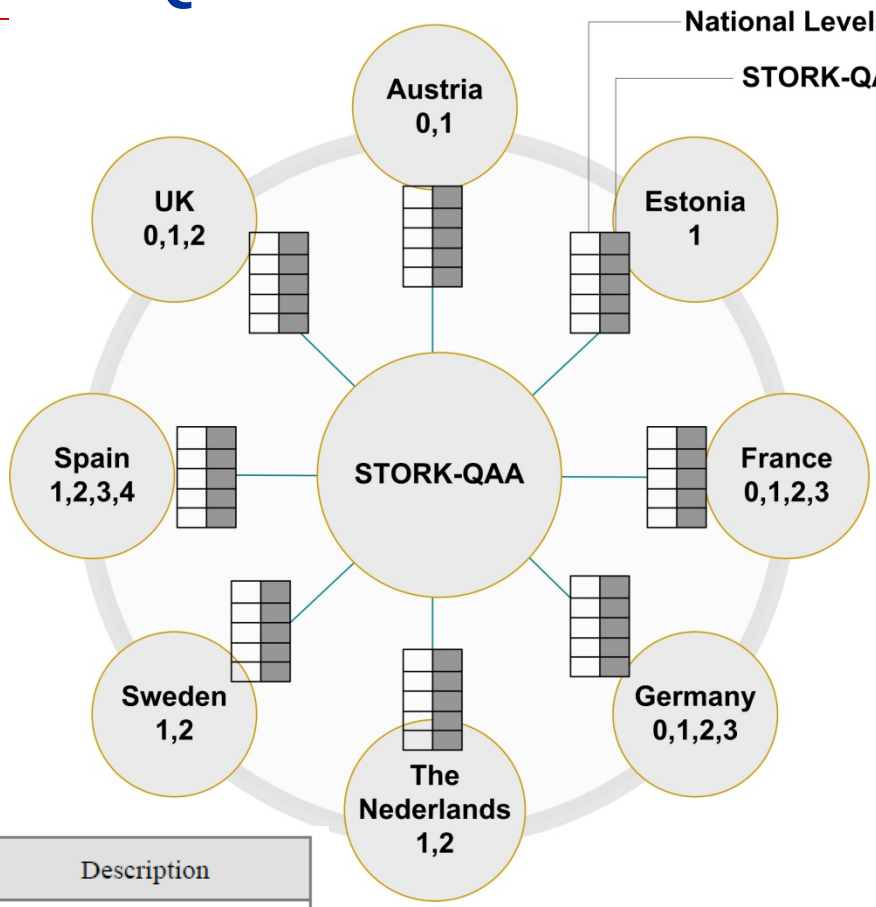


Different technologies and security levels:

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

Approach: Mapping to QAA levels

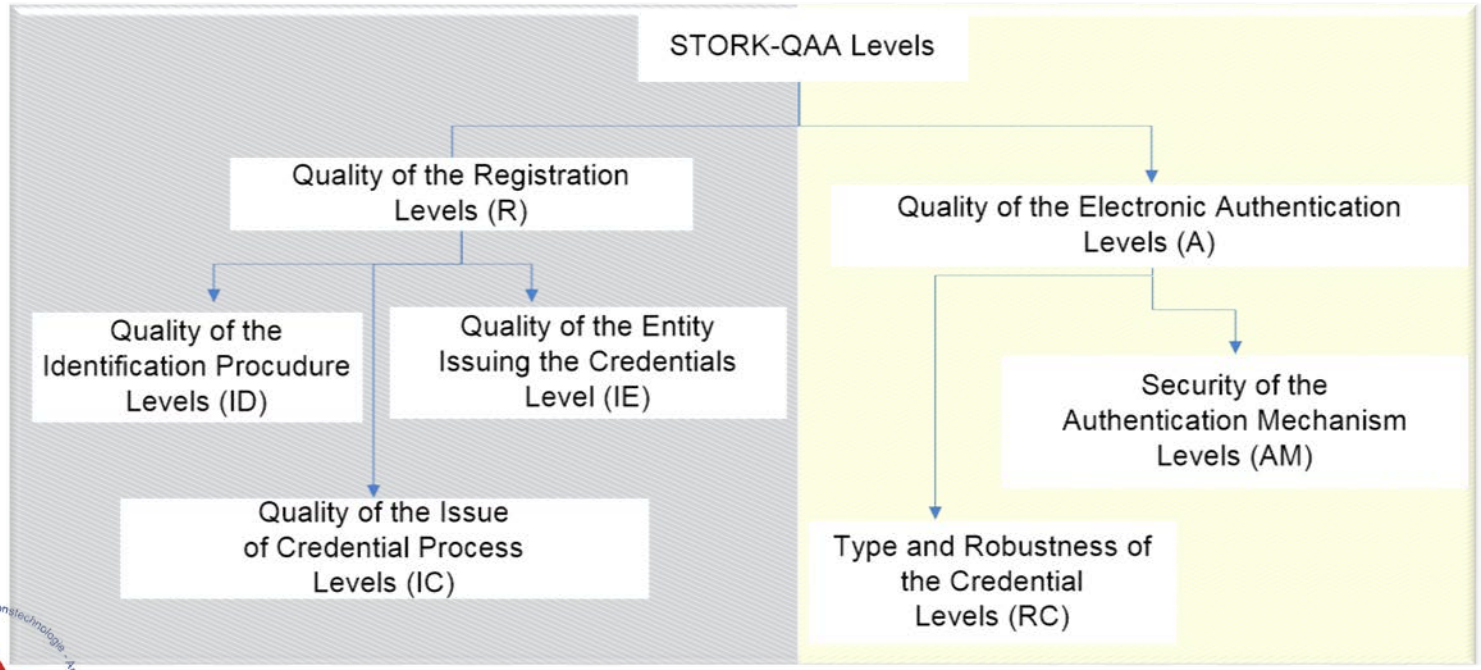




STORK QAA level	Description
1	No or minimal assurance
2	Low assurance
3	Substantial assurance
4	High assurance

QAA: Security - Assurance

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



```
100 --------------------------------
110 REM EUKLIDISCHER ALGORITHMUS
120 REM IN TURBO-BASIC
130 REM FUER WIKIPEDIA VON FLUPS
200 --------------------------------
210 INPUT "A: ",A
220 INPUT "B: ",B1
300 --------------------------------
310 A=A1:B=B1
320 WHILE B<>%0
330   IF A>B
340     A=A-B
350   ELSE
360     B=B-A
370   ENDIF
380 WEND
400 --------------------------------
410 ? "GGT(";A1;",";B1;")=";B
420 --------------------------------

READY
```

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)**

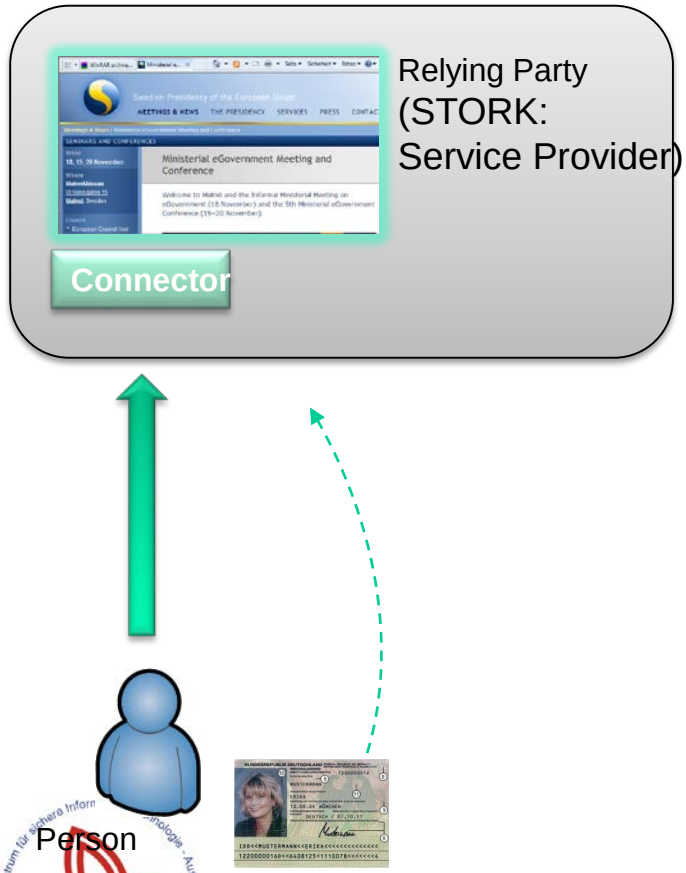
.. and combine them (*MW⇨MW, PEPS⇨PEPS, MW⇨PEPS, PEPS⇨MW*)

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

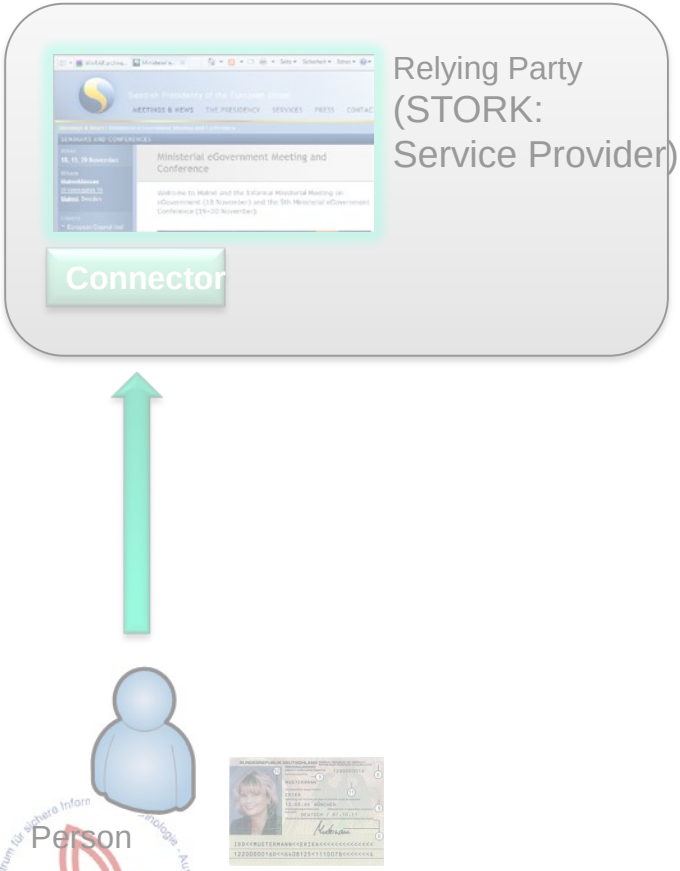
Direct Authentication



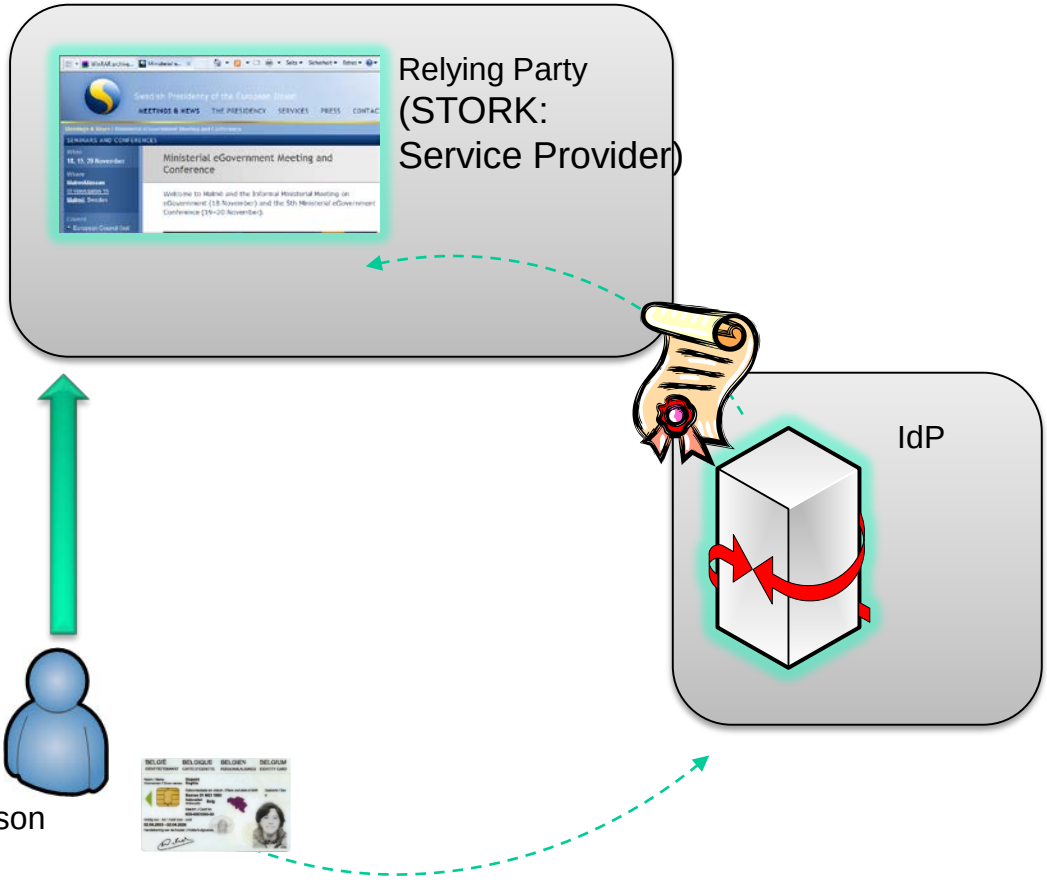
Direct vs. Indirect authentication

Replay from section 5

Direct Authentication



Indirect (IdP-based) Authentication

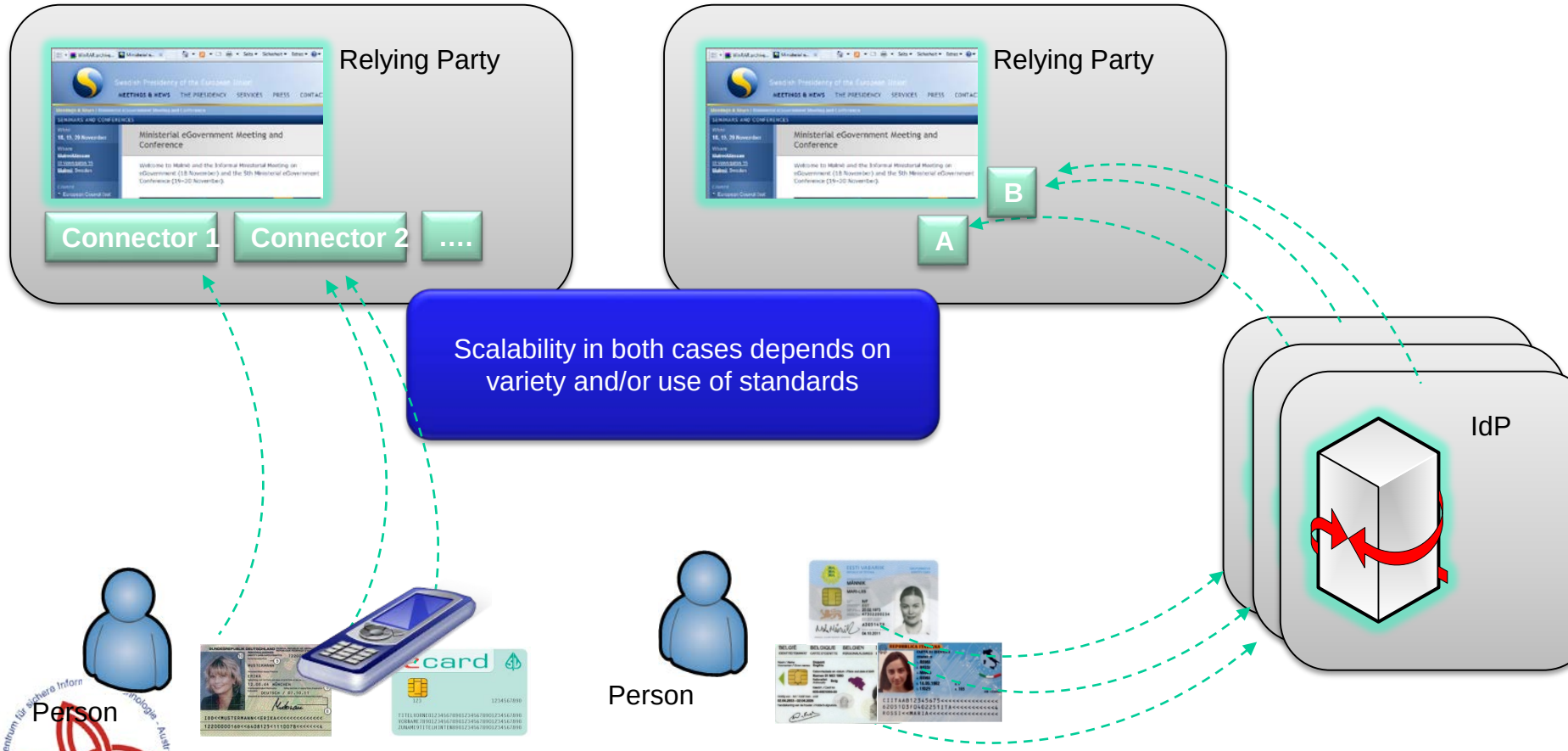


Direct vs. Indirect authentication

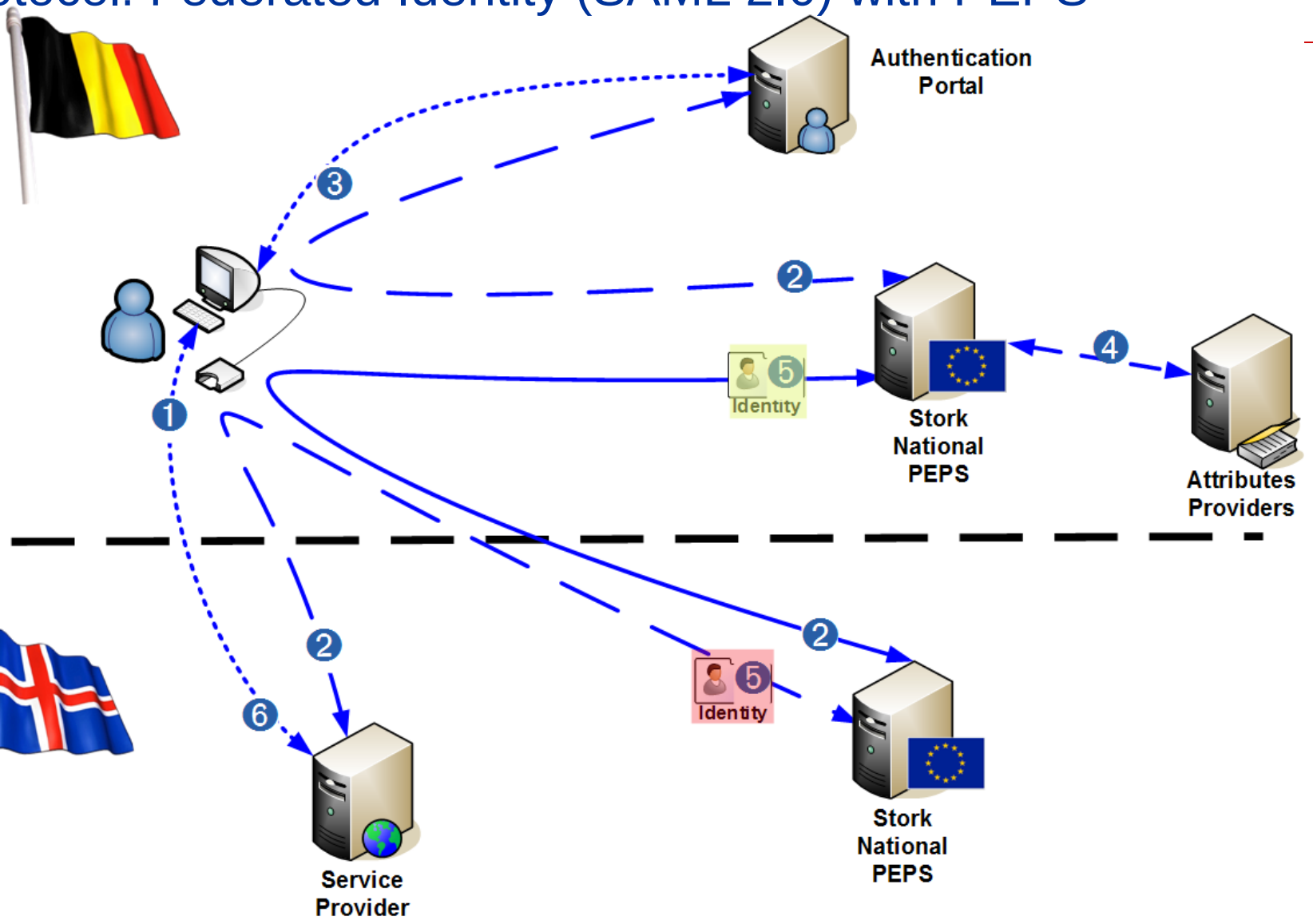
Replay from section 5

Direct Authentication

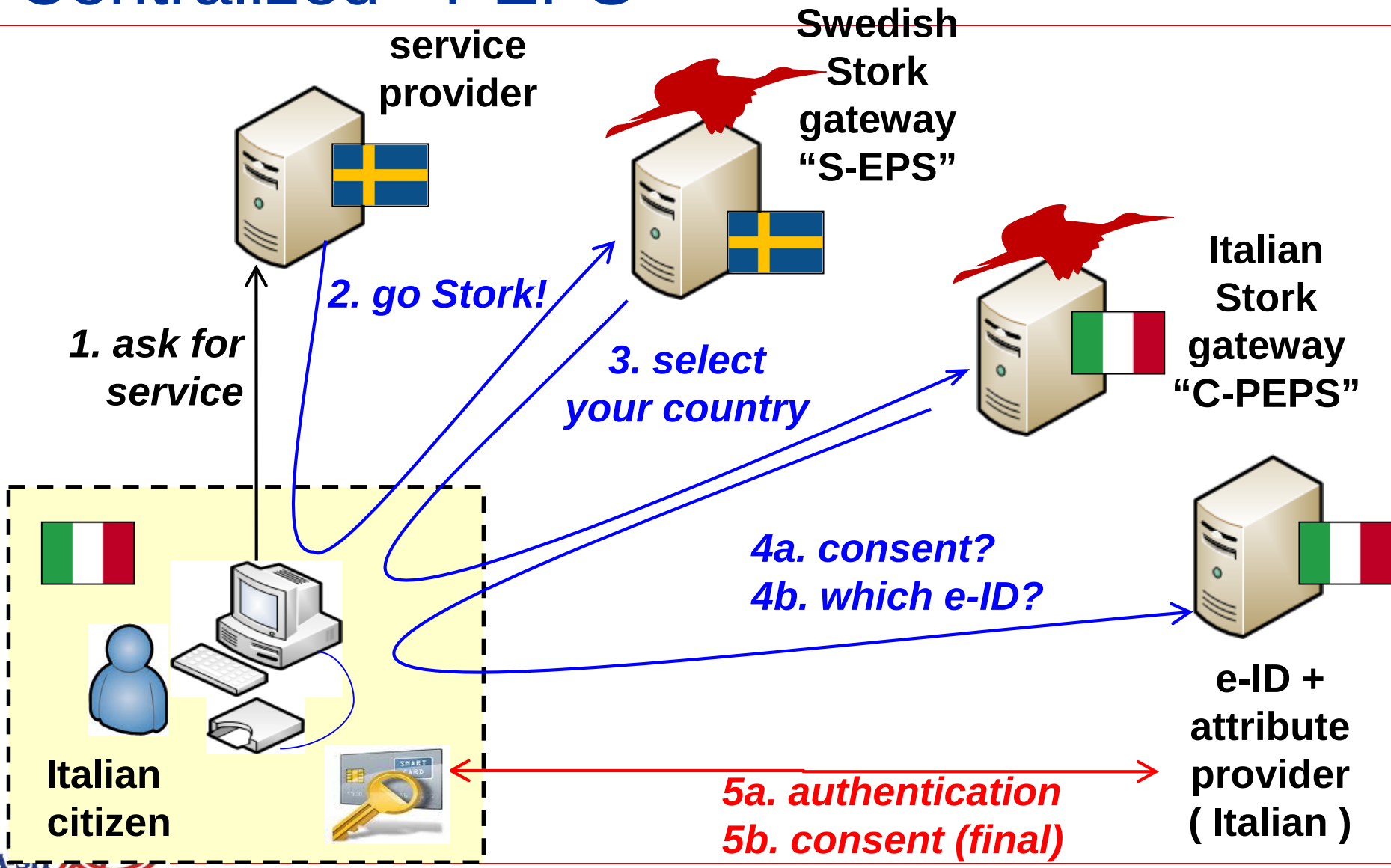
Indirect (IdP-based) Authentication



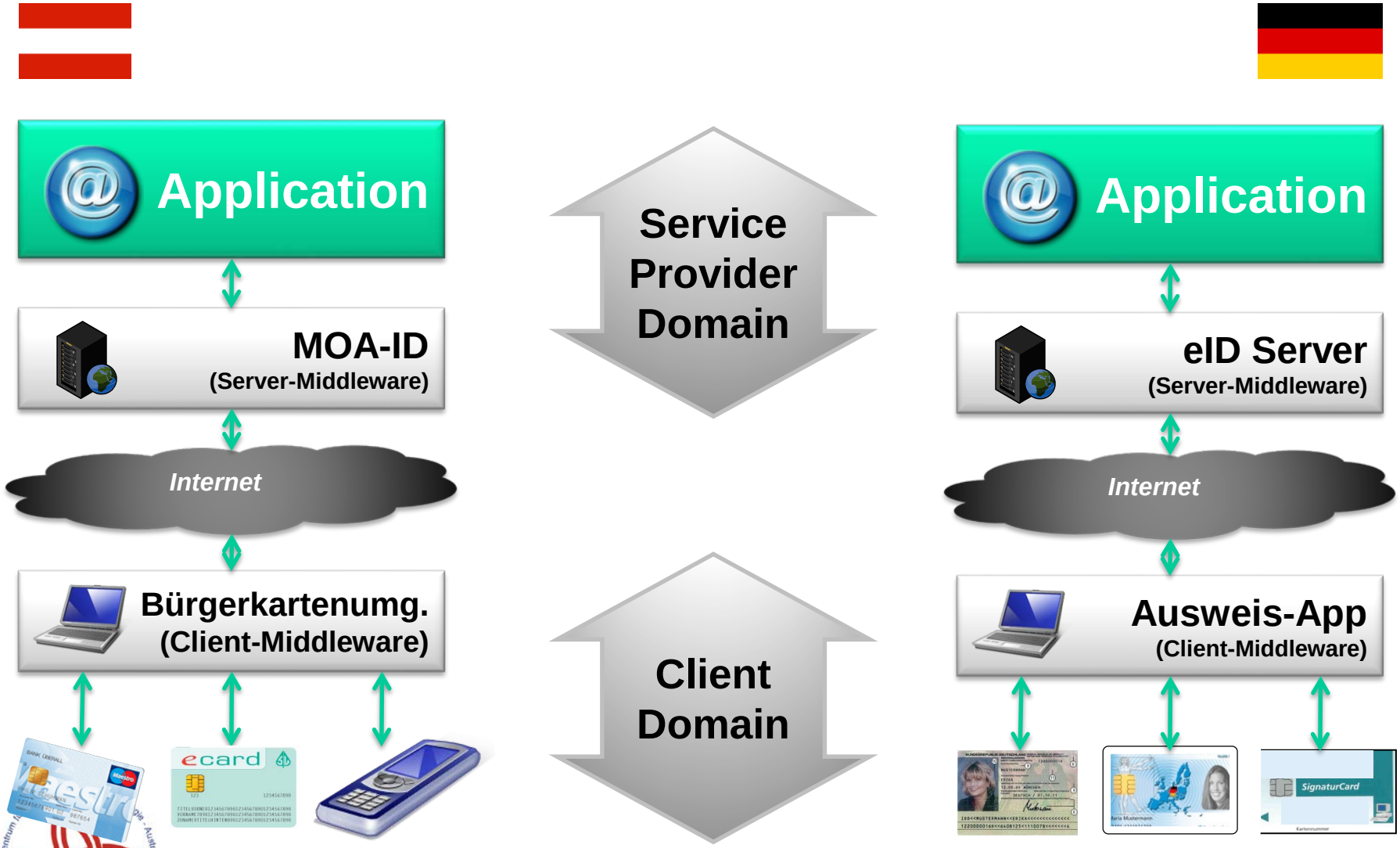
Protocol: Federated Identity (SAML 2.0) with PEPS



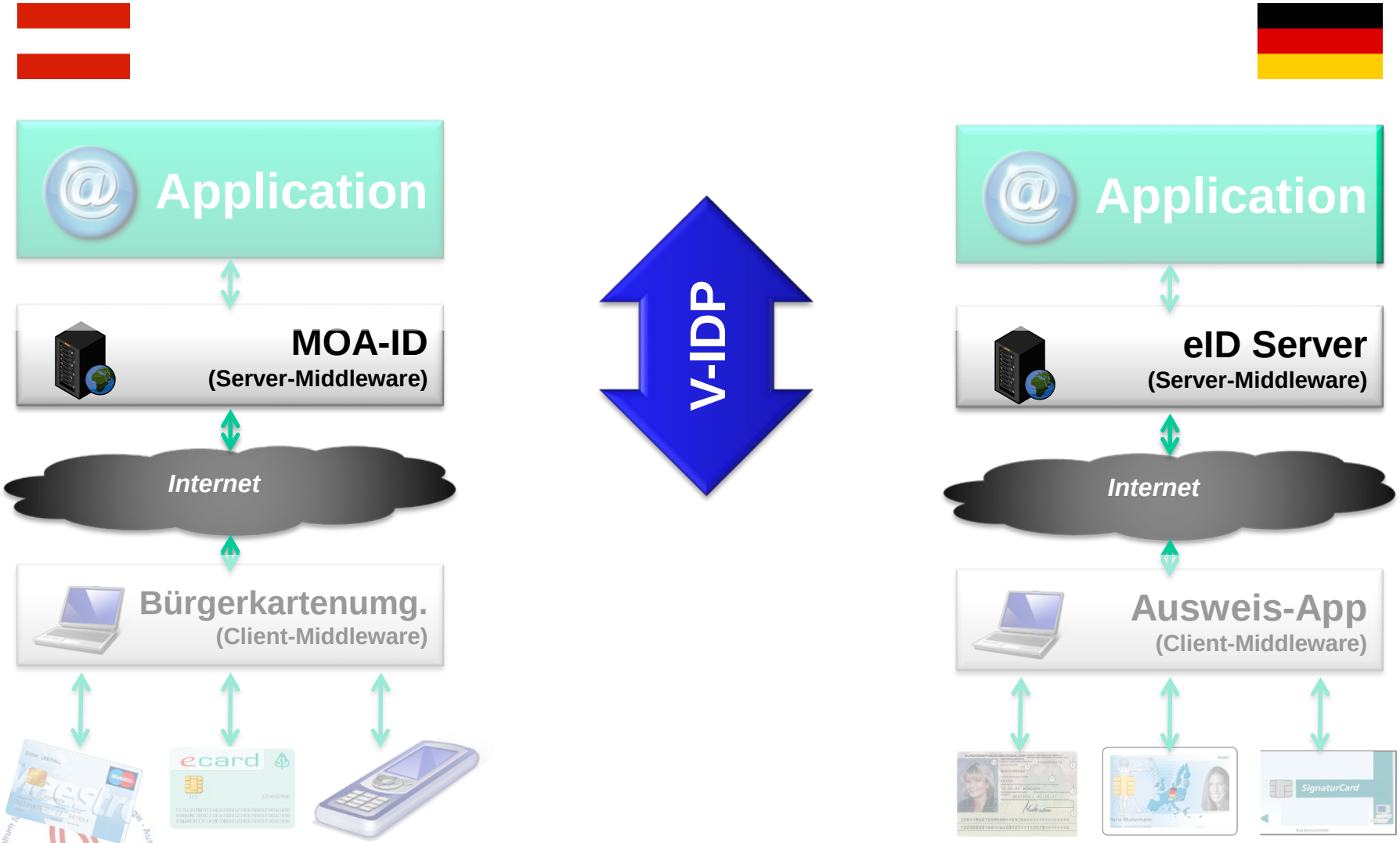
Centralized - PEPS



Decentralized – Middleware Approach



Decentralized – Common Middleware / Virtual-Identity Provider



PEPS Architecture

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

Two major parts

- 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

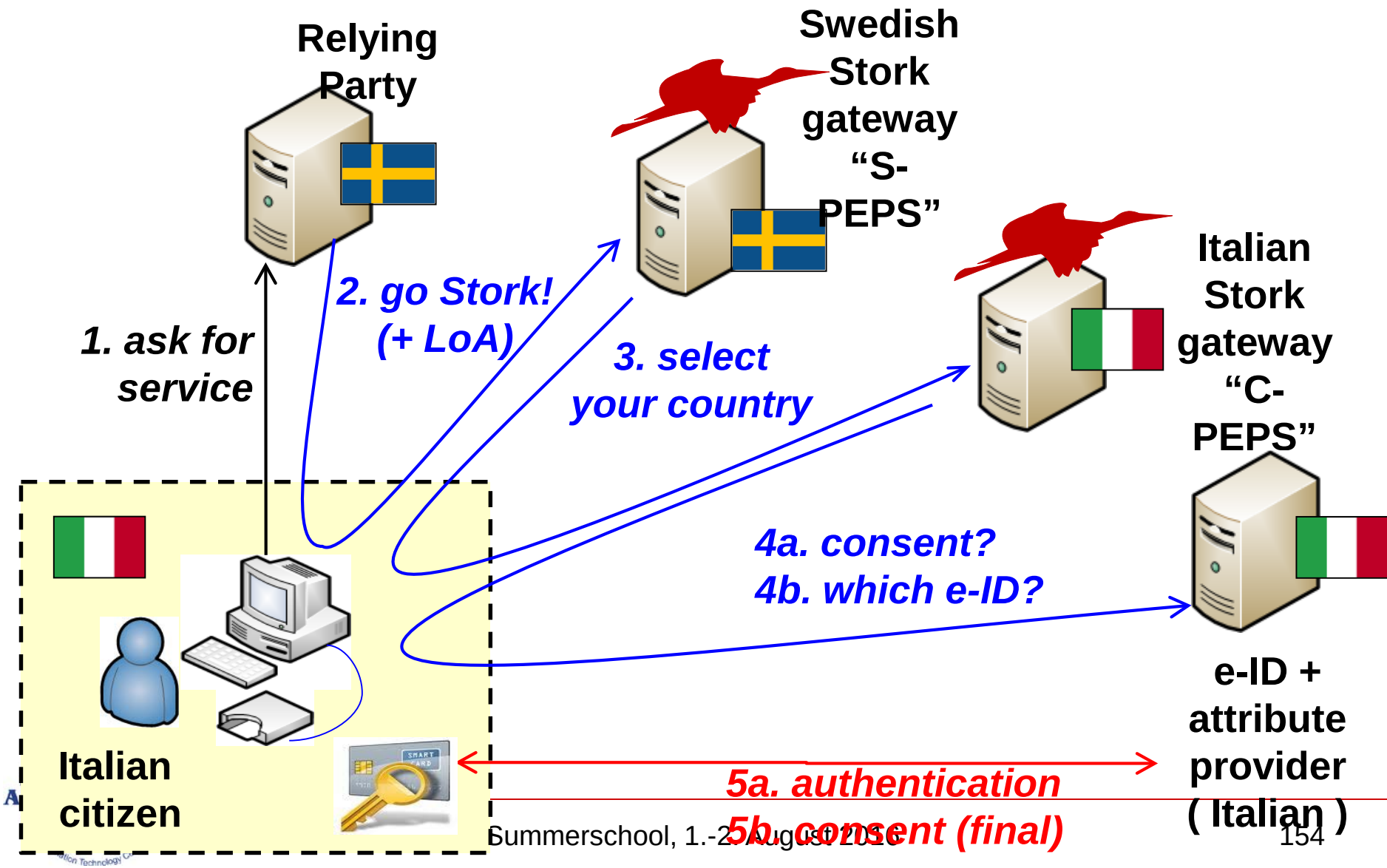
- Reference V-IDP
  - √ Java 1.5
  - √ Application Servers - Enterprise application
    - Glassfish V2
    - jboss
    - Weblogic

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?

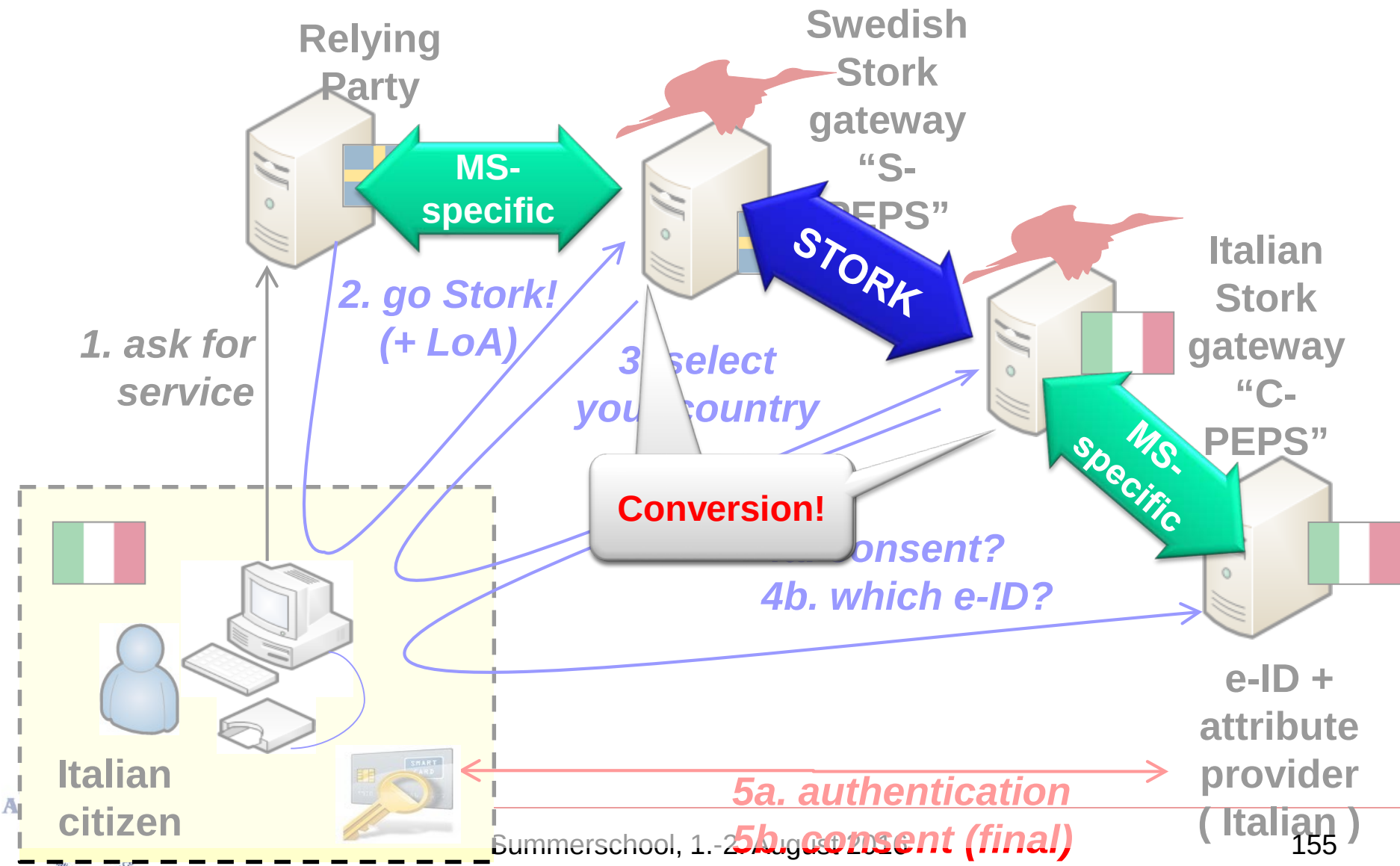
Centralized – PEPS Process

common STORK and MS-specific parts



Centralized – PEPS Process

common STORK and MS-specific parts

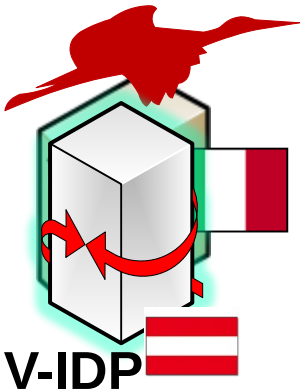


PEPS-VIDP Process

Austrian accessing Swedish Relying Party

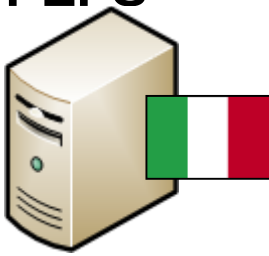
Relying Party

Swedish Stork gateway "S-PEPS"

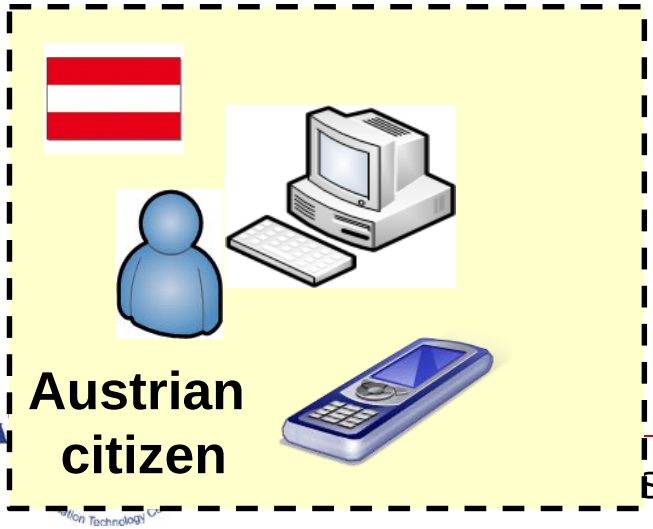


V-IDP

Italian Stork gateway "C-PEPS"



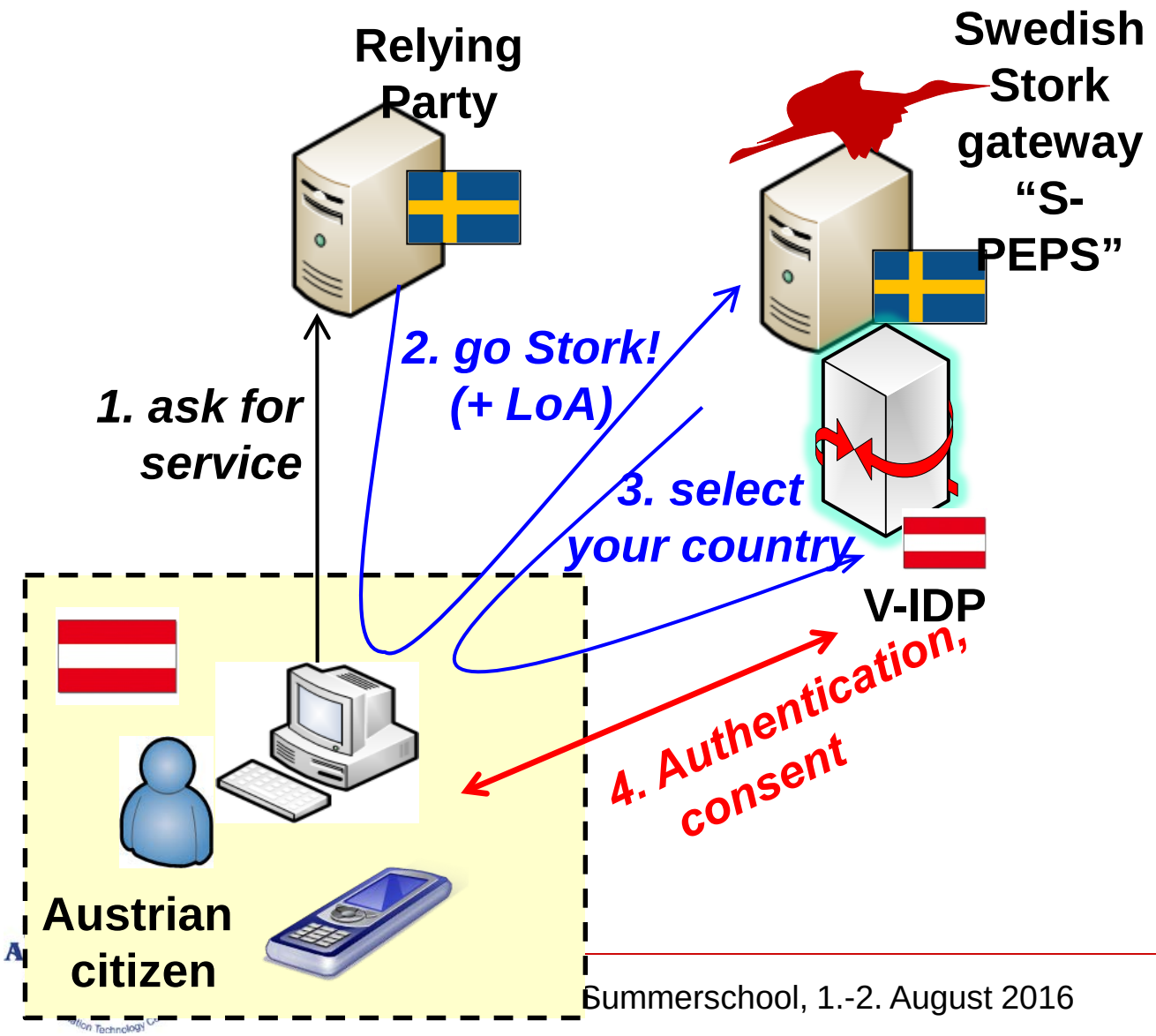
e-ID + attribute provider (Italian)



Austrian citizen

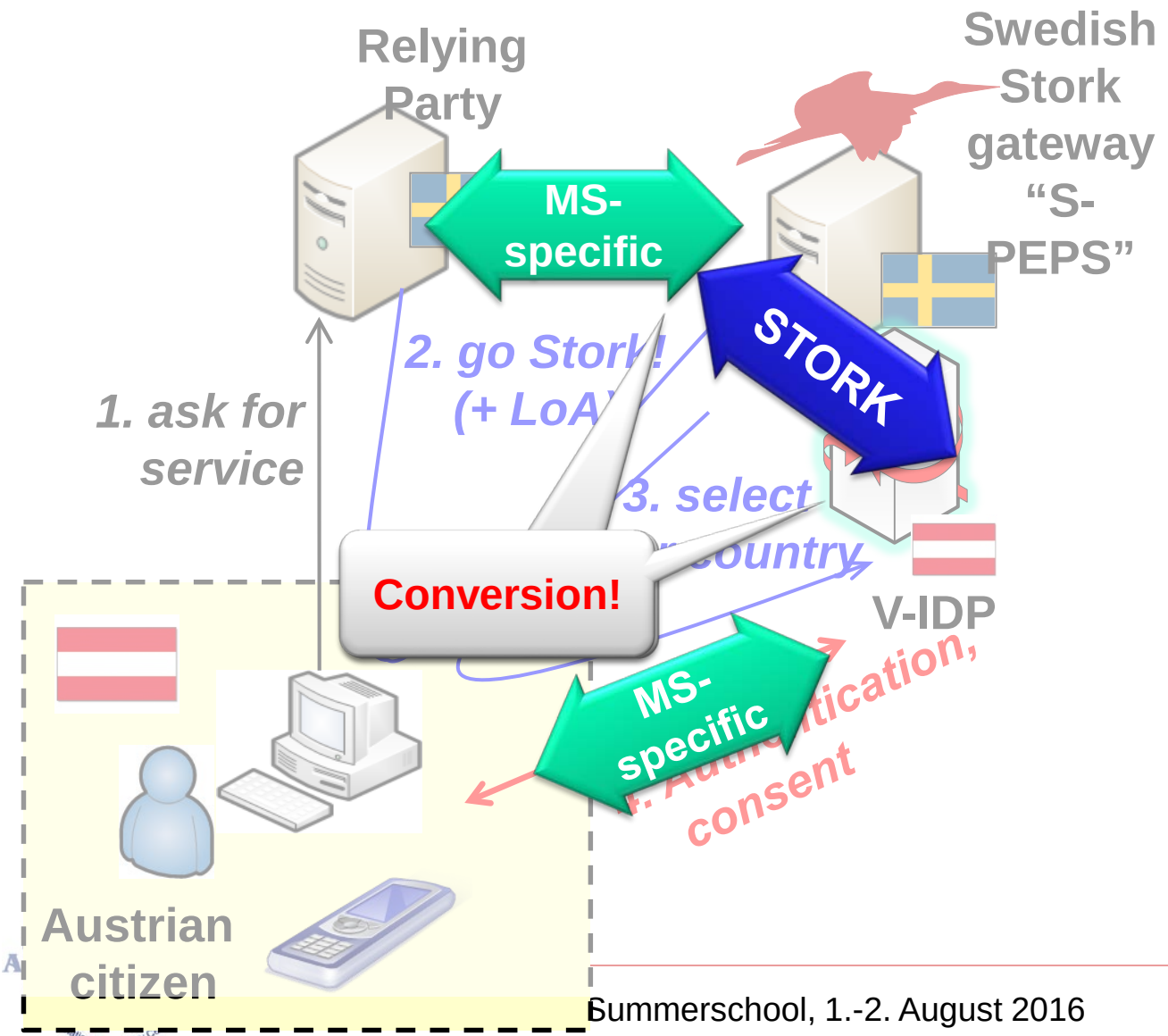
PEPS-VIDP Process

Austrian accessing Swedish Relying Party



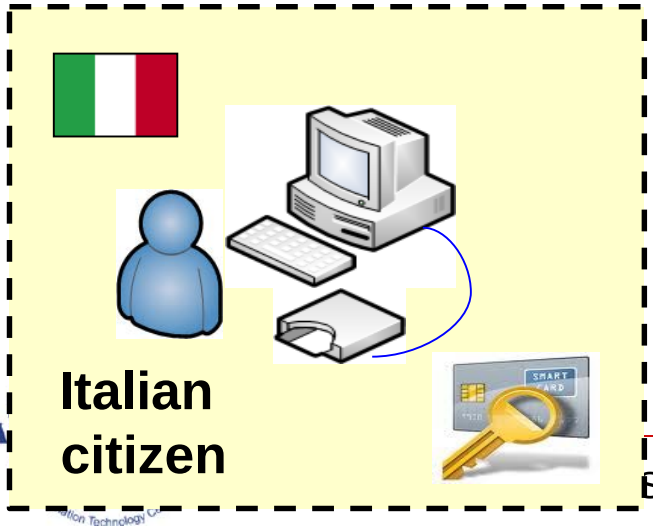
PEPS-VIDP Process

common STORK and MS-specific parts



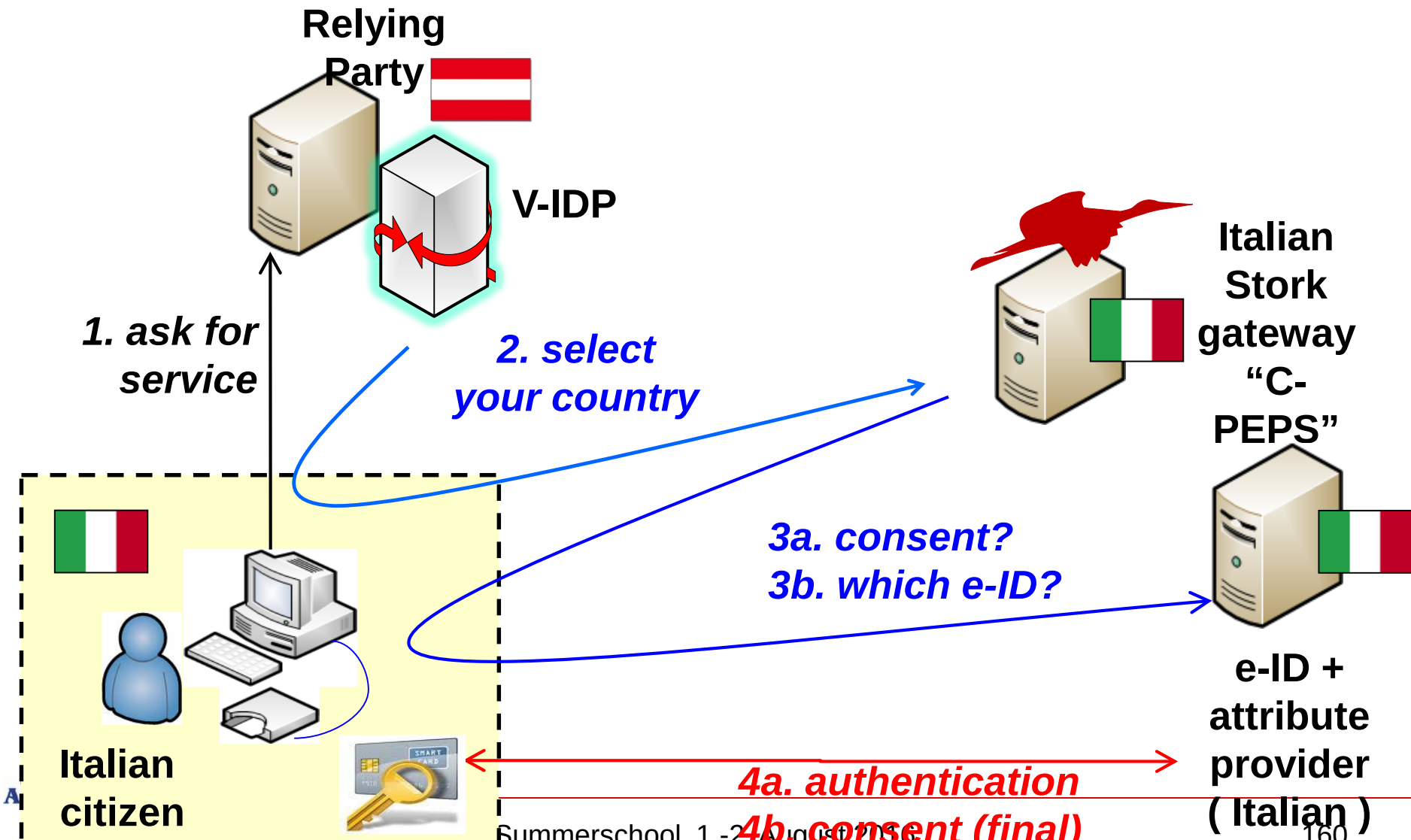
VIDP-PEPS Process

Italian accessing Austrian Relying Party



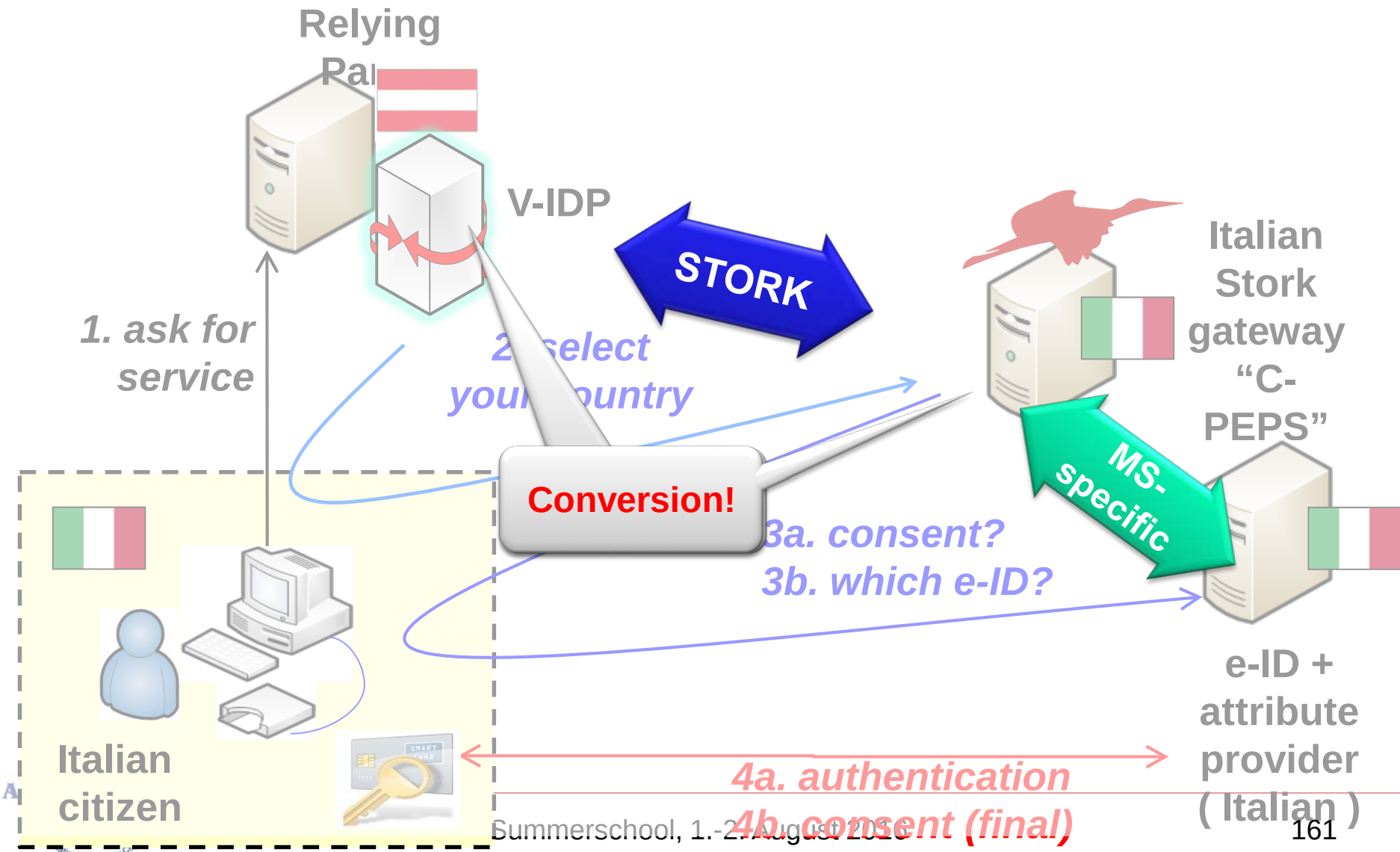
VIDP-PEPS Process

Italian accessing Austrian Relying Party

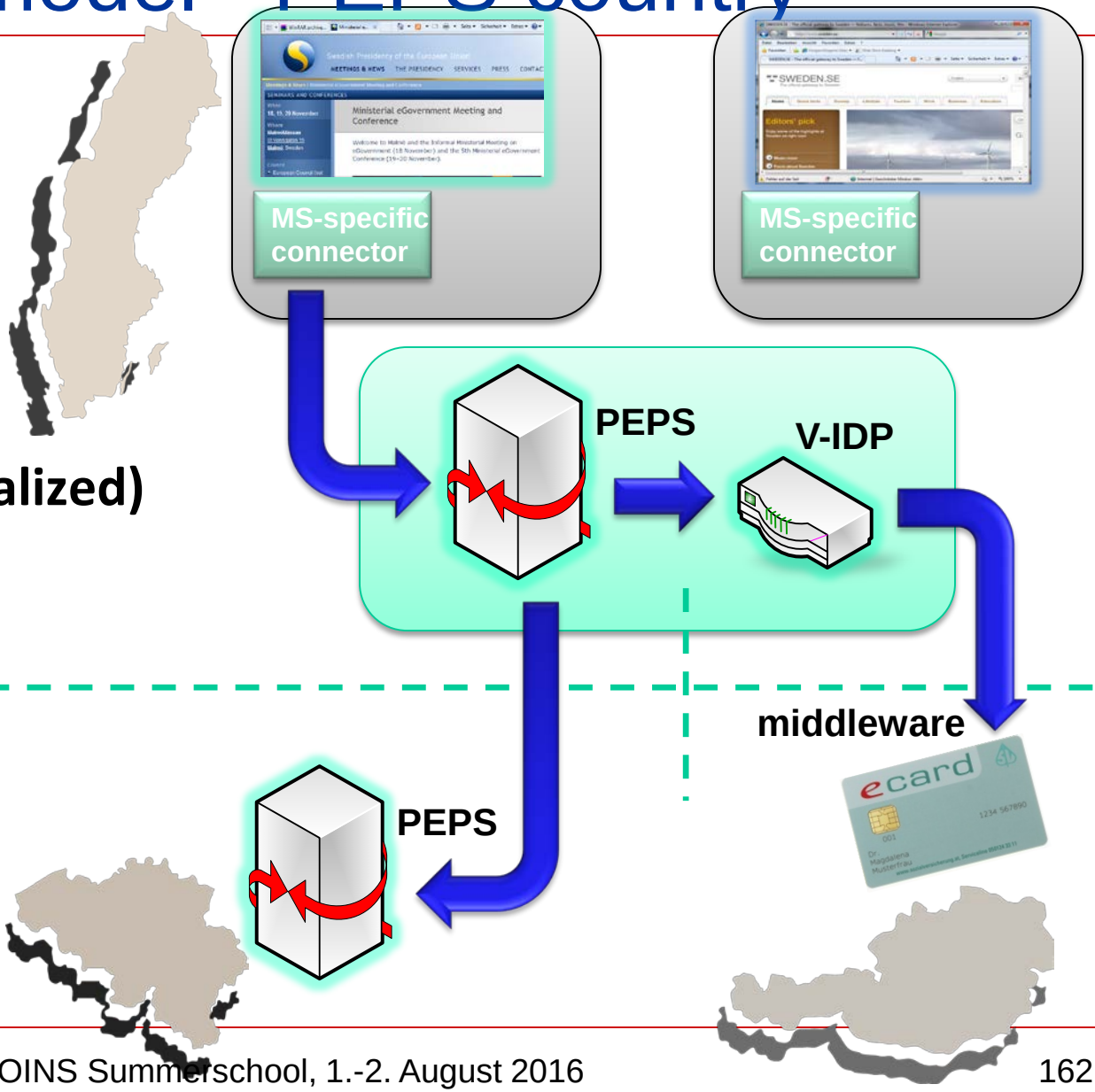


VIDP-PEPS Process

common STORK and MS-specific parts

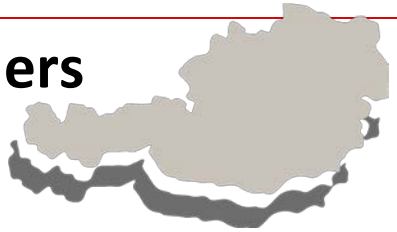


Integration model "PEPS country"



Integration model "MW country"

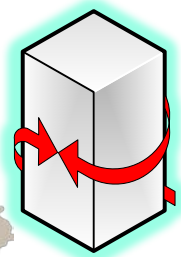
Service providers

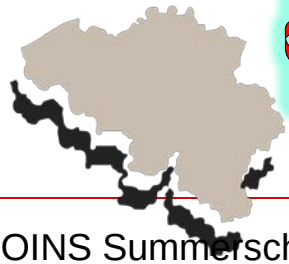


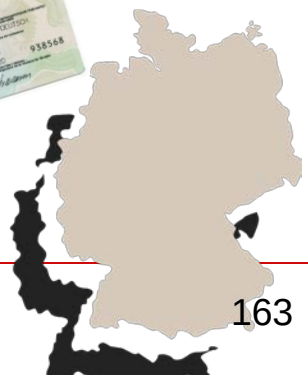
STORK Layer (decentralized)

middleware

Foreign eID







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

isa 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

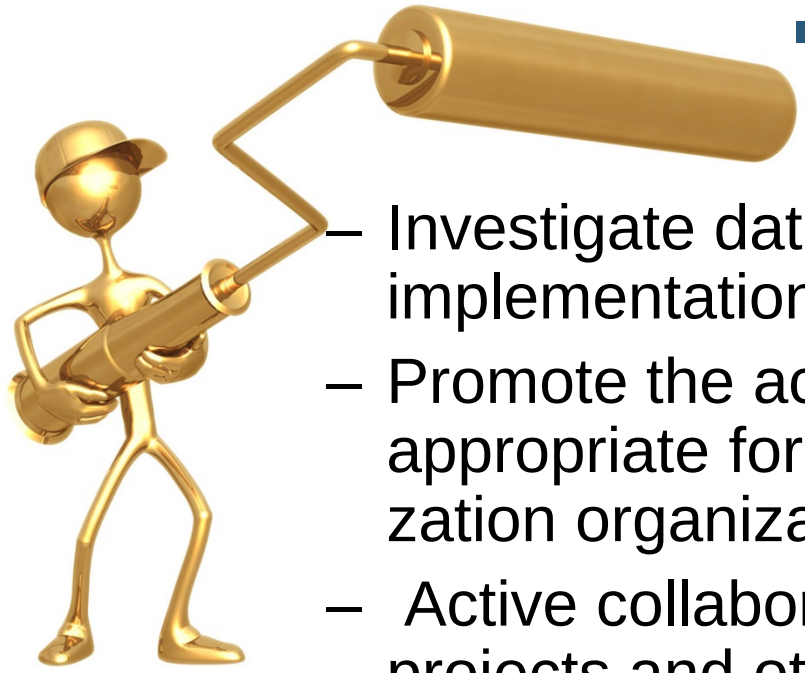
To get grip on governance (I/II)

- 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.

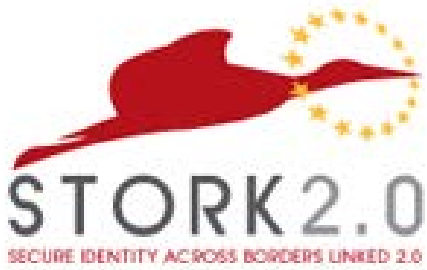
To get grip on governance (II/II)

- 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

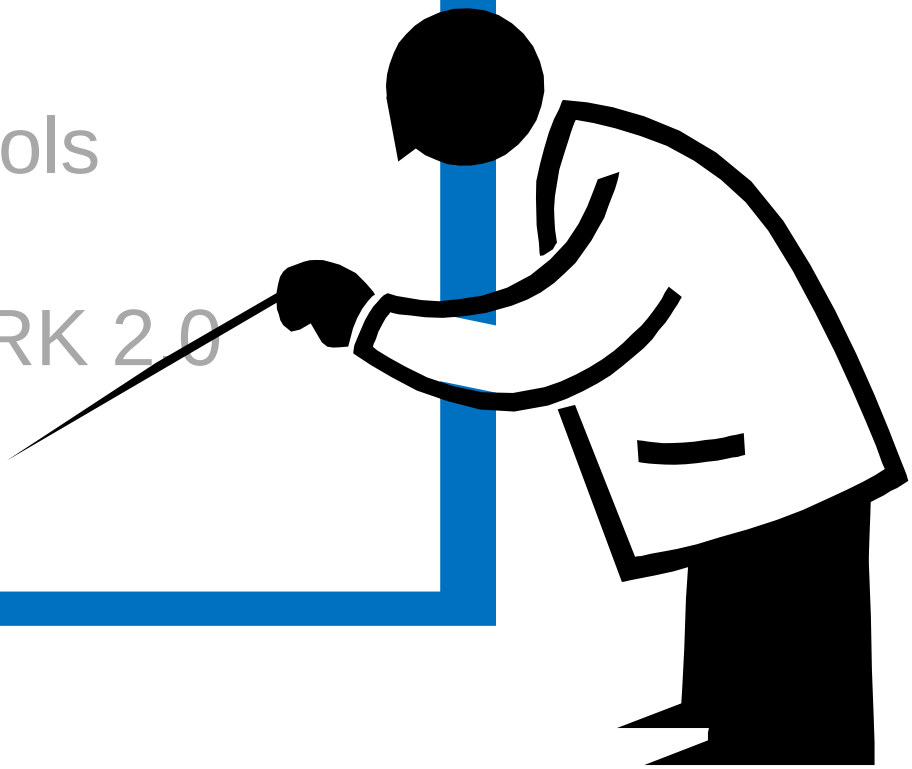
Demos

- Authenticate at European Commission Services

- Authenticate as legal re-presentative of a company

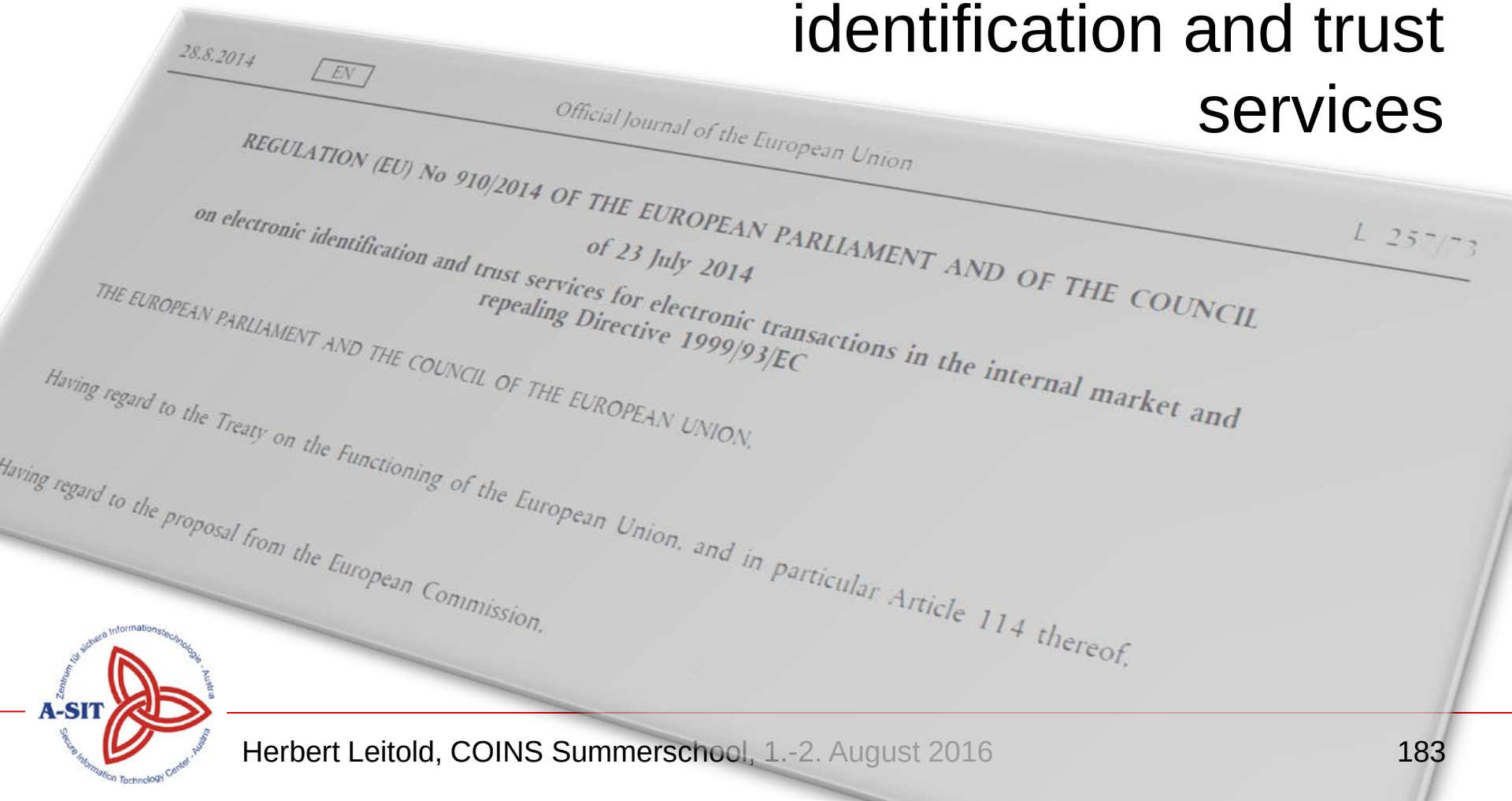
Contents

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

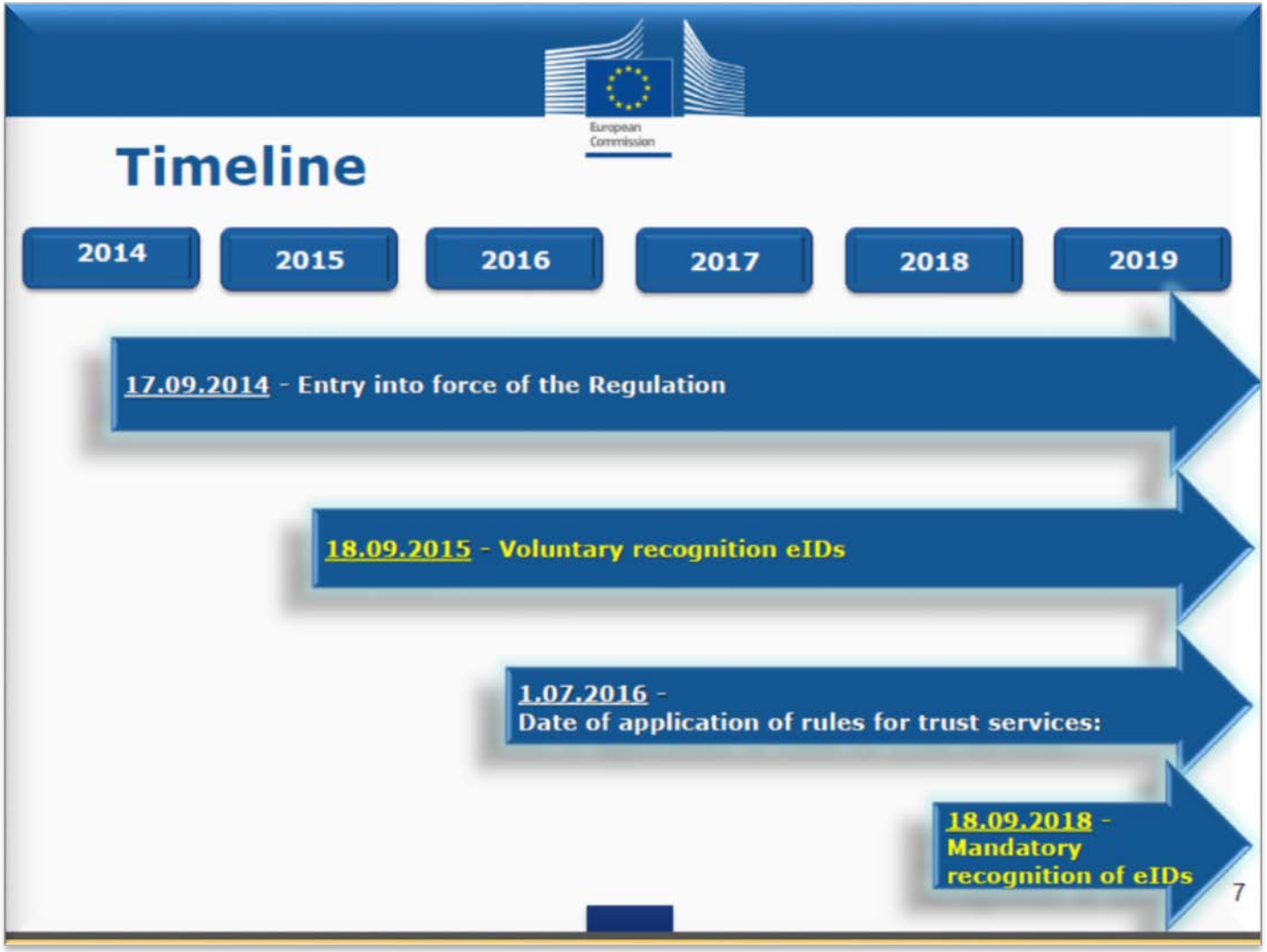
MS sovereignty, but recognition obligation
(Coordination on interoperability and security)

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

eIDAS Trust Services

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

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 high attack potential

LoA – Management and Organisation

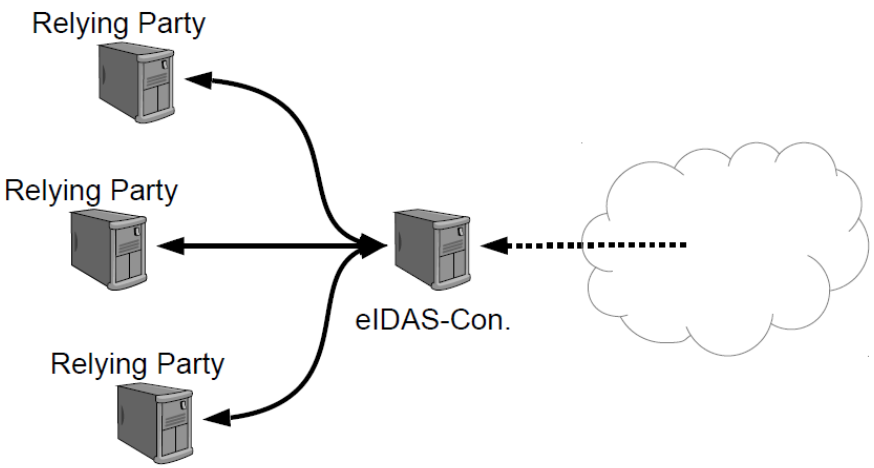
- Ensure that documented information security management practices, policies, approaches to risk management, and other recognised controls are in place
- Requirements on record keeping, facilities, staff, technical controls, etc.
- Most of these managerial and organisational requirements equally apply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

eIDAS Technical Specifications

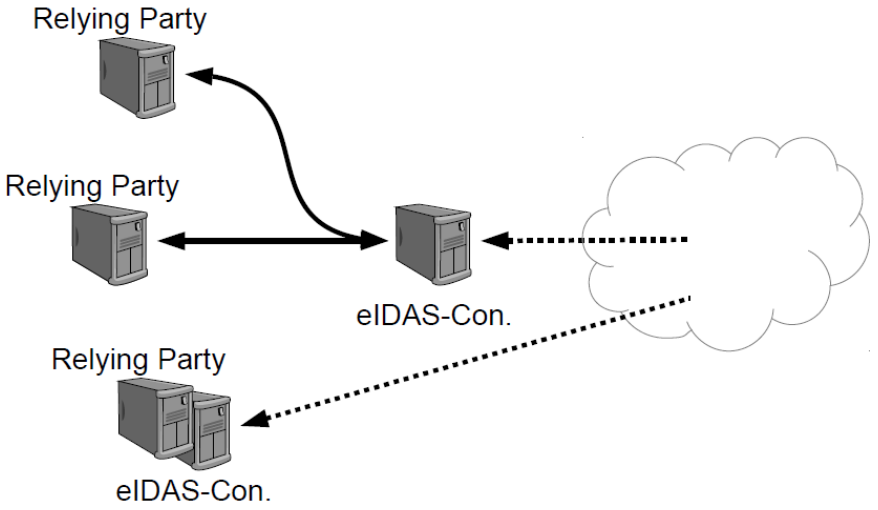
1. Interoperability Architecture
   - Overview, General Requirements
2. Message Format
   - SAML 2.0 Profile
3. Attribute Profile
   - Minimum Data Set based on ISA Core Vocabulary
4. Crypto Requirements
   - Crypto Suites for TLS and SAML

ad “1. Interoperability Architecture”

- Options at receiving MS



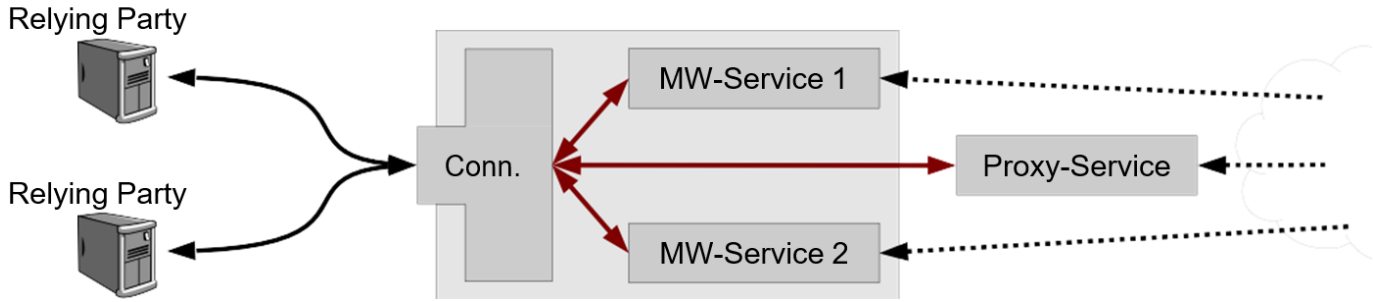
Centralized MS



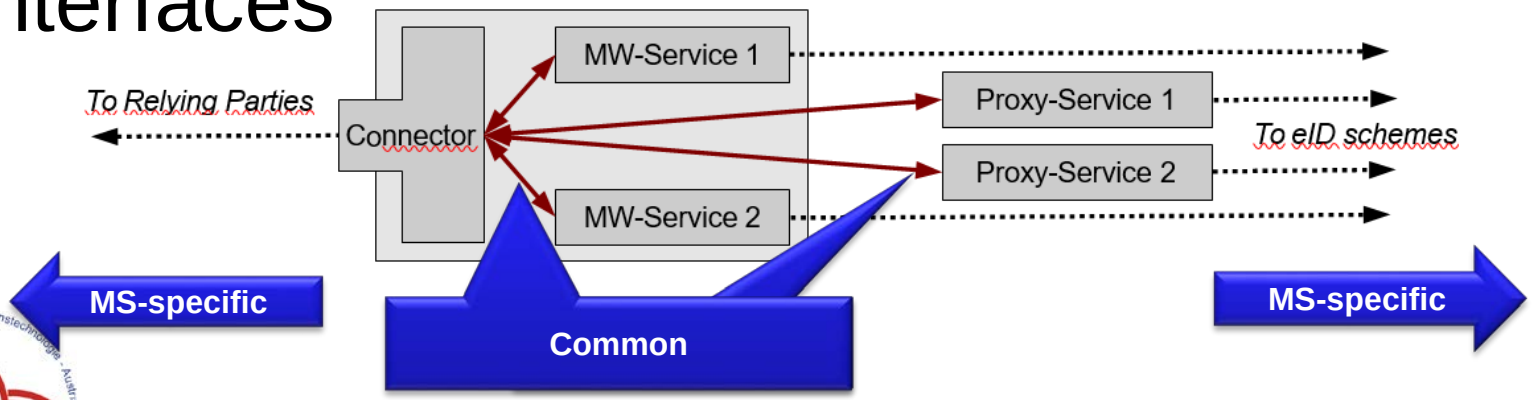
Decentralized MS

ad “1. Interoperability Architecture”

- Receiving MS components

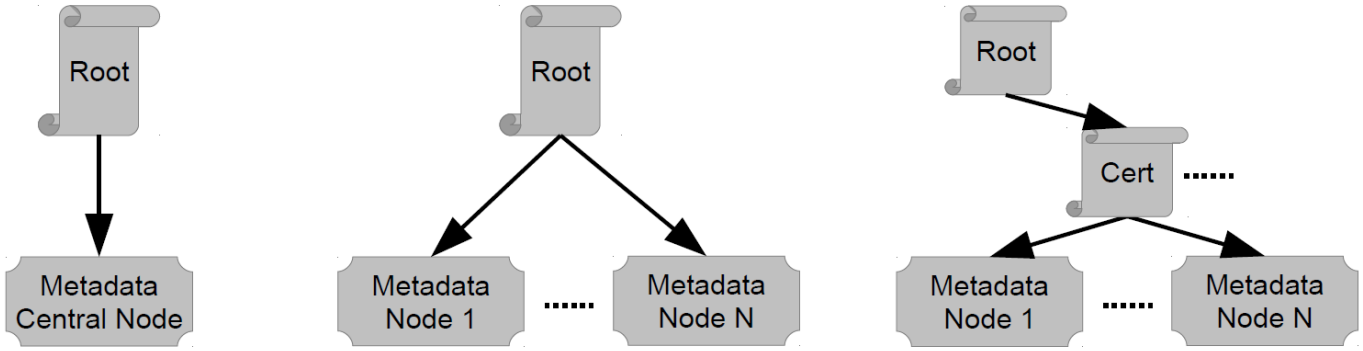


- Interfaces



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"/>
<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>
<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>
<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>
<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>
```

POST or –REDIRECT Request to that URL

A unique ID, …

the family name, …

the first name, ….

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

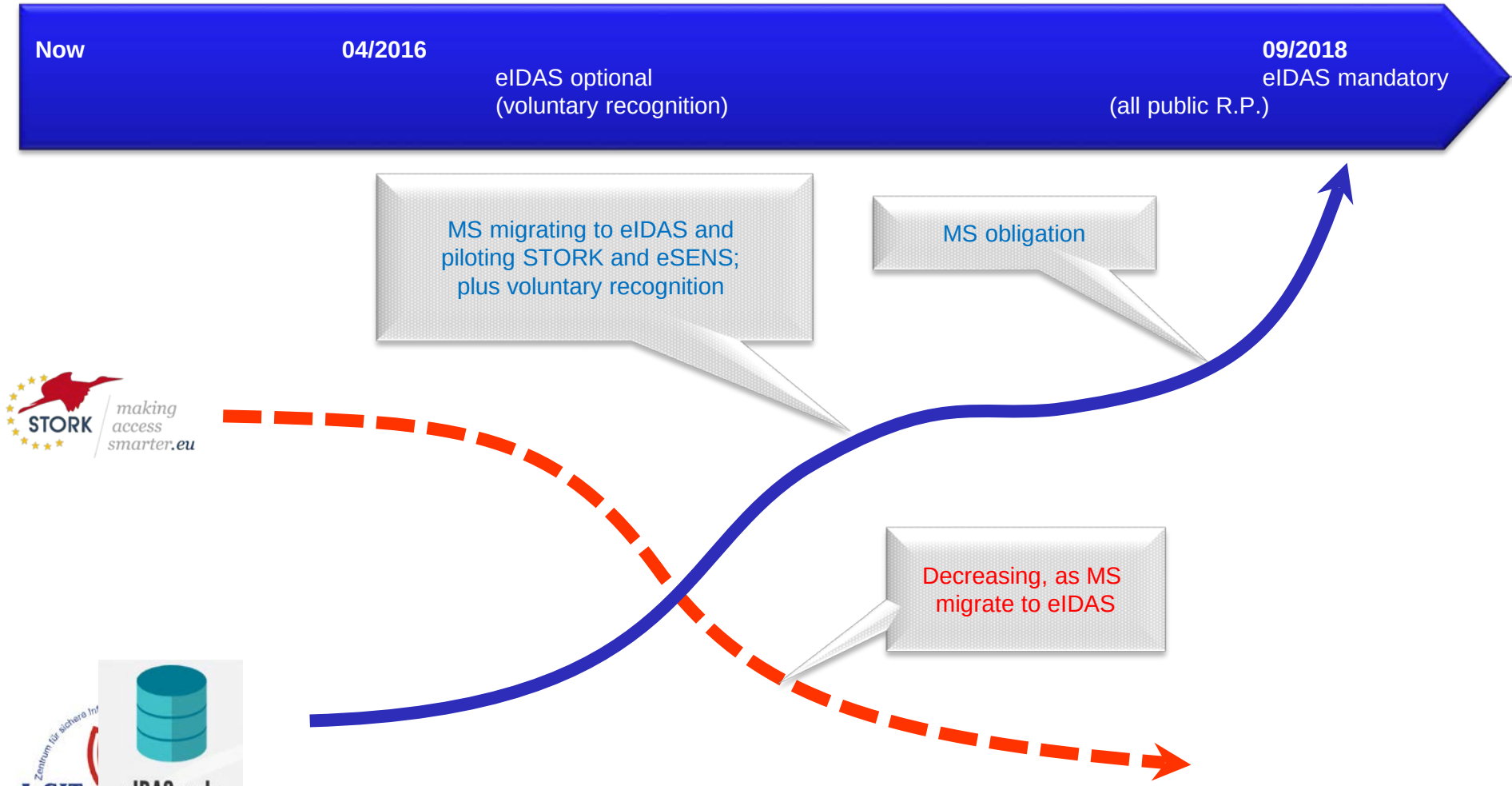
https://ec.europa.eu/cefdigital

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

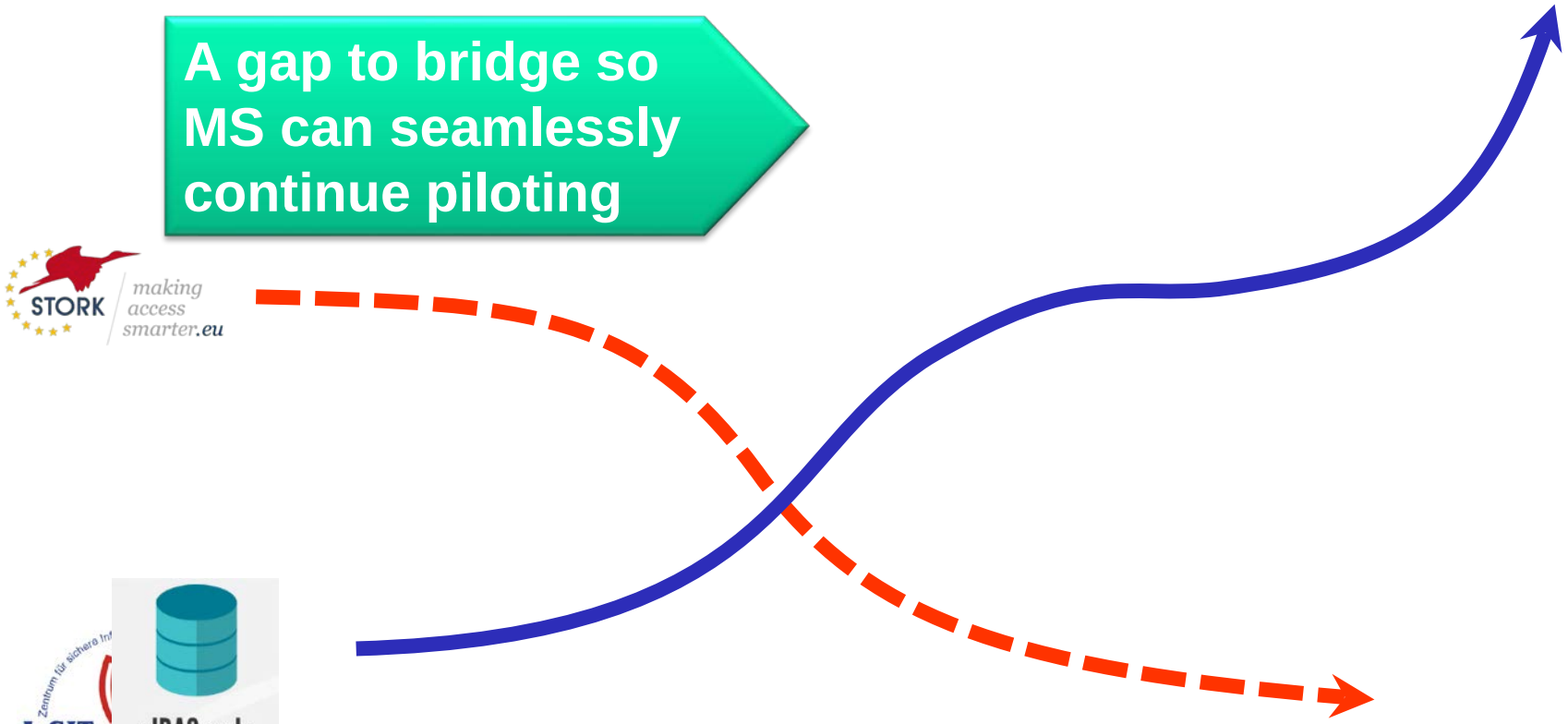
Protocols are not compatible

Expected infrastructure evolution



How are Service Providers affected?

A gap to bridge so MS can seamlessly continue piloting



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!