STORK PRESENTATION

SECURE IDENTITY ACROSS BORDERS LINKED

Challenges of eID interoperability:
What we learn(ed) from the STORK journey?

Primelife Summerschool, Helsingborg, 3.8.2010

Herbert.Leitold@egiz.gv.at

Stork is an EU co-funded project INFSO-ICT-PSP-224993

Presentation Overview

- eID motivation, a little history
- STORK Project Environment
- Interoperability Models and Integration
- Technology

ID - what if something goes wrong …

- Digital twins, identity theft, …

Government eID projects …

- Early birds started late 1990's early 2000

Finish eID card: December 1999

Estonian eID card: from January 2002

Austrian citizen card: from 2003, mass-rollouts 2005

Italian CIE / CNS: test phase 2003 (CIE)

Belgian eID card: from 2nd half 2003

Government eID projects …

- Early birds started late 1990's early 2000

– Finish eID card: December 2002

– Estonian eID´card: from January 2002

– Austrian citizen card: from 2003 mass-rollouts 2005

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

– Belgian eID card: from 2nd half 2003

Evolved as national islands

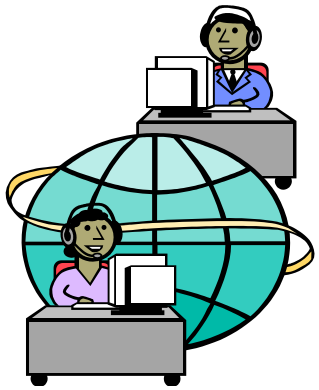
National eIDs landscape

- Heterogeneous in various dimensions
  - Technology
    - Smartcards: AT, BE, EE, ES, FI, GE, IT, PT, SE, …
    - Mobile eID: AT, EE, FI, LU, NL, NO, UK, …
    - Soft certif.: ES, SE, SI, …
    - usern./pass.: NL, UK, …
  - Operational
    - Issued by public sector, private sector, combined
    - Issued at federal, local, regional level
    - Use of identifiers
  - Legal
    - (Limited) use of identifiers; flat, sectoral, combi

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

Cross-border cases

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

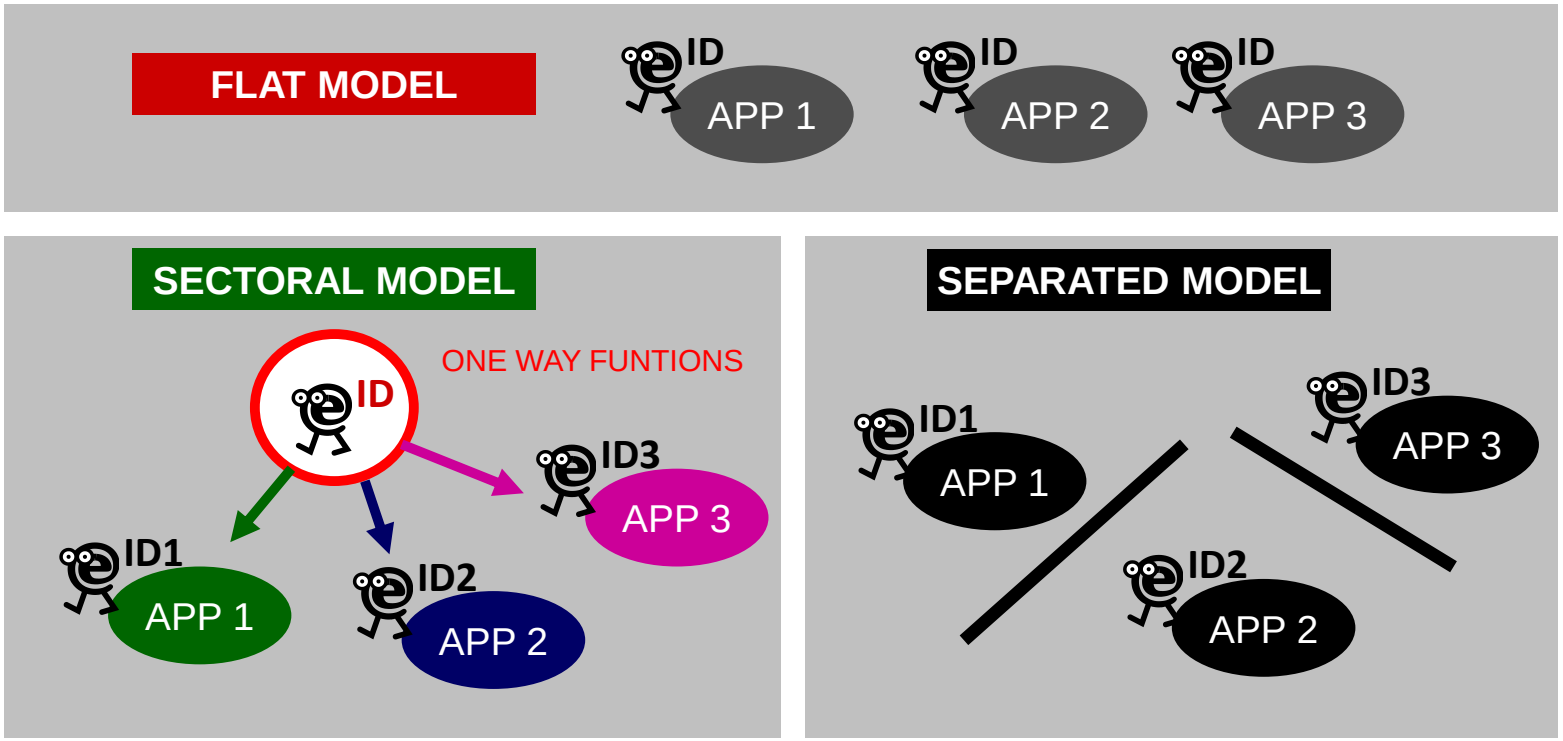


… and many, many more private sector applications!

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

A little history: eID ad-hoc-group *(2004-2005)*

… discussed the identifier models of MS

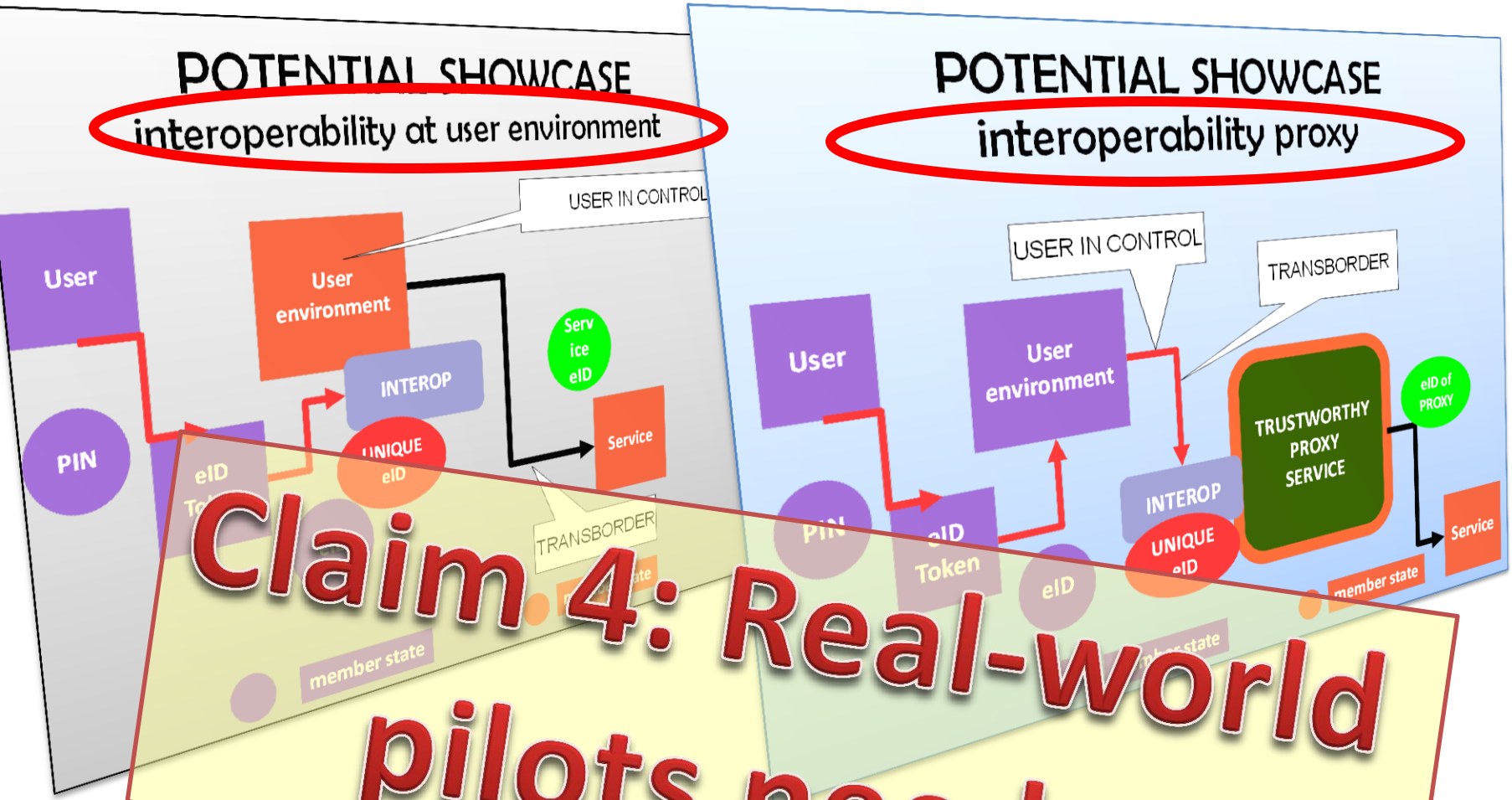


A European eID model must coexist with all three models not :: compromising privacy

eID MUST NOT ADD ADDITIONAL PRIVACY RISKS TO EXISTING APPLICATIONS

A little history: eID ad hoc-group *(2004-2005)*

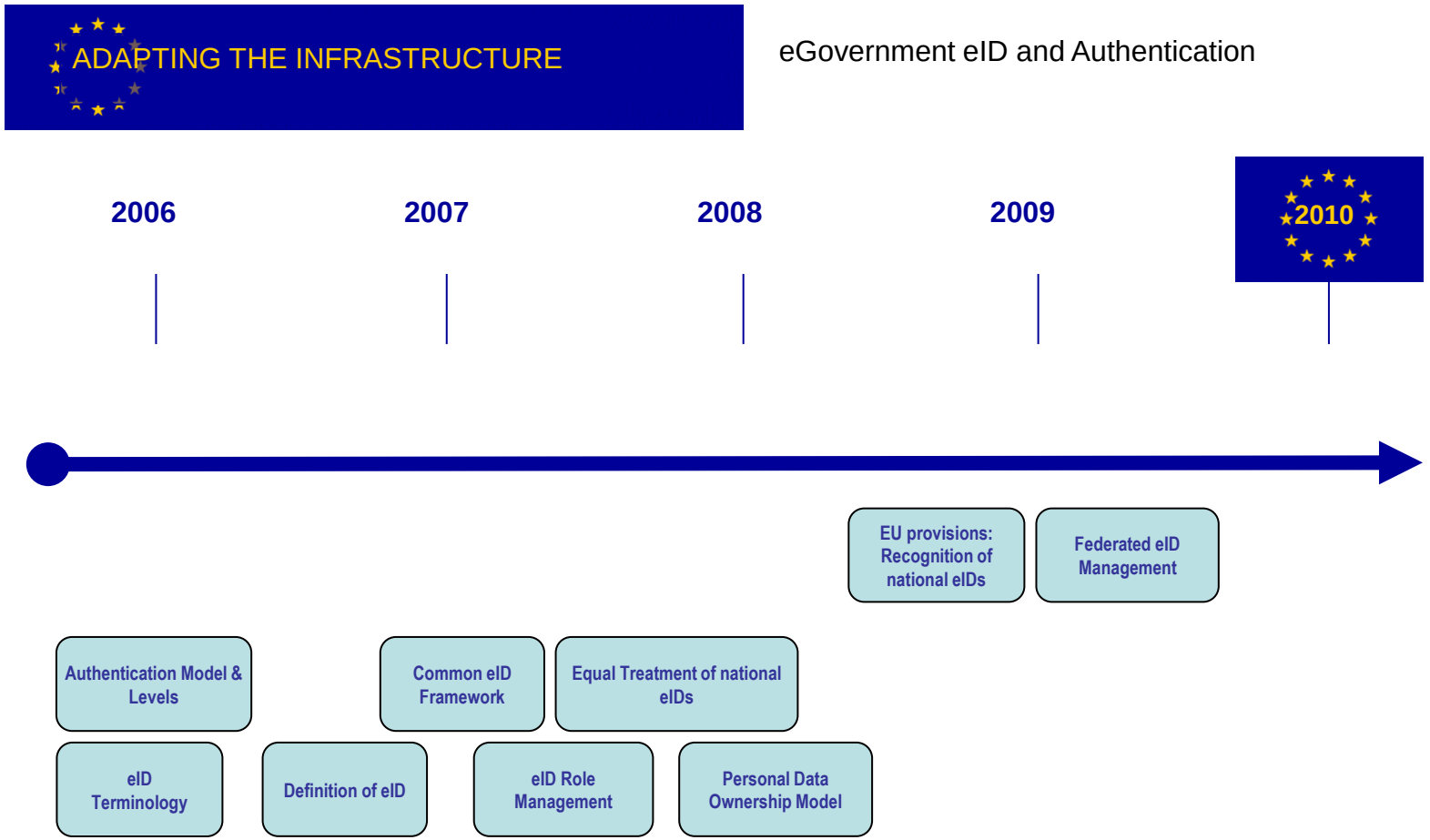
… discussed possible interoperability models



Claim 4: Real-world pilots needed

A little history: eID ad hoc-group *(2004-2005)*

… developed signposts with a roadmap



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

eIDs in STORK (*those piloting in 1st phase*)

Country & sec. level		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.)*
Iceland	2	yes	-	-	all	all	-	yes
Italy	2	yes	-	-	all	all	yes	yes (sig.-card)
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	yes (QAA 3-4)	yes (QAA 4)	yes (QAA 3-4)	yes (QAA 3-4)
Sweden	12+	yes	-	yes	-	*tbc*	yes	yes

Presentation Overview

- ✓ eID motivation, a little history
- STORK Project Environment
- Interoperability Models and Integration
- Technology

eGovernment objectives (ICT-PSP call 2007)

Type A

- eProcurement
- **eID interoperability**
- eHealth

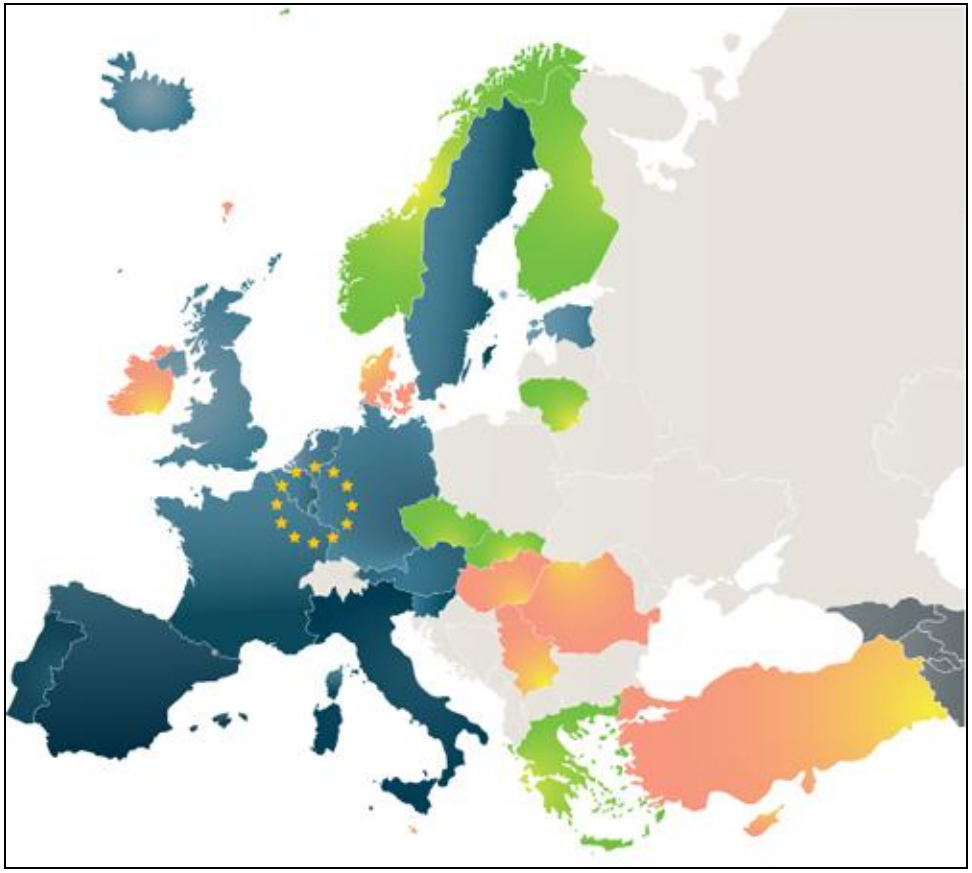
Type B

- Electronic documents
- Accessible & inclusive eGovernment
- Combined delivery of social services

Thematic Networks

- eParticipation
- Impact & user satisfaction
- Brokering pan-EU eGov solutions & services online

STORK – Member State involvement



Member States/EEA – STORK

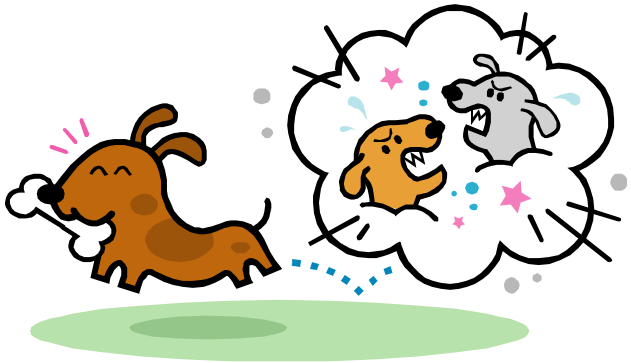
Member States Ref Group

STORK-2 (original plan)

The Basis

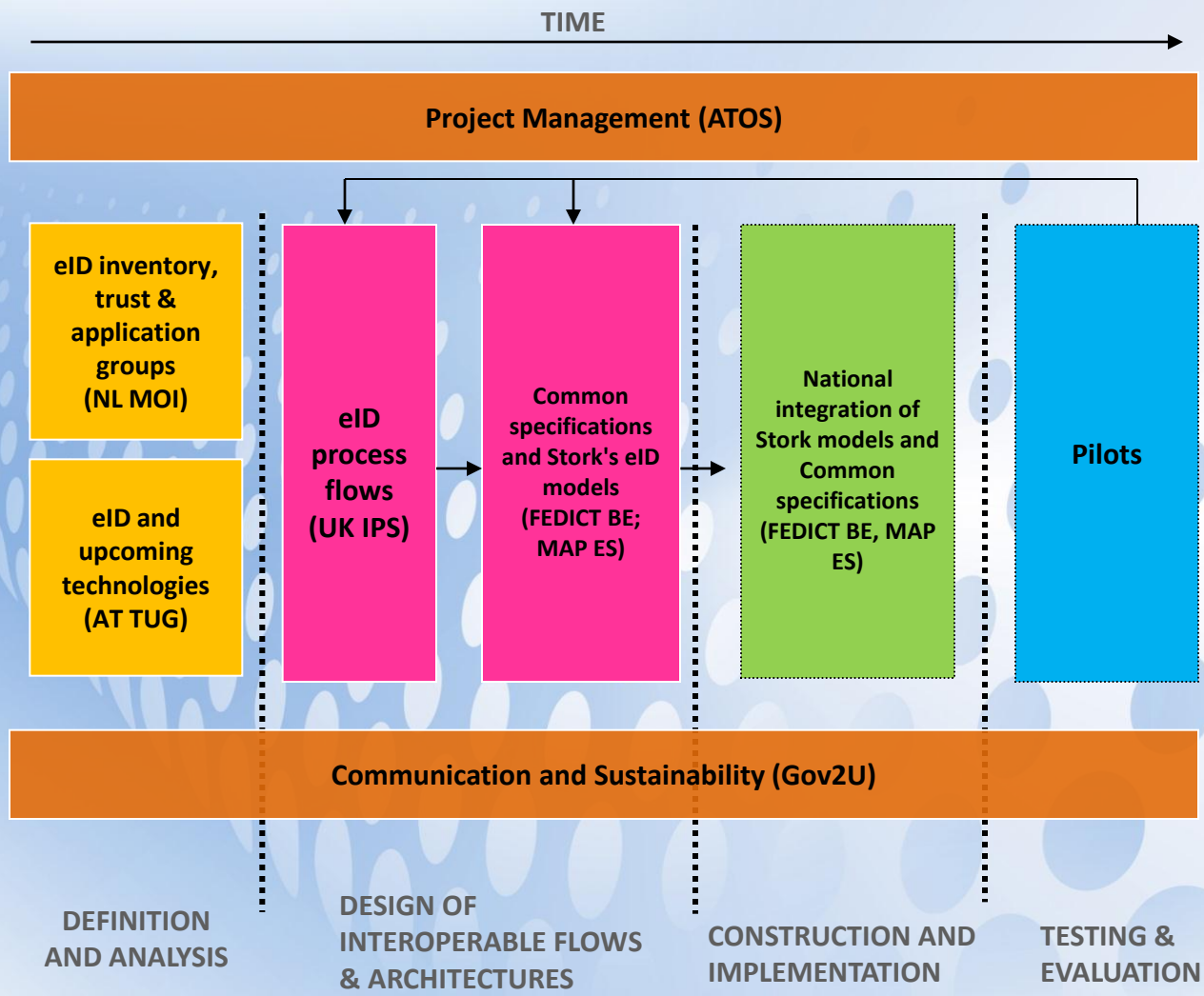
- Member States have eID projects
  - planned, deploying, or operational
- Heterogenous environment
  - Technology: smartcards, username/passwords
  - Operational: e.g. centralized, decentralized
  - Legal: e.g. persistant identifiers, sector-specific IDs
- STORK does not change the MS situation, but aims at interoperability on top of it

Issues to be tackled



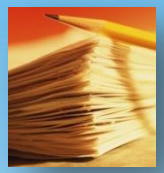
- Consensus needed
- Legal
  - e.g. MS limit use of national identifiers
  - can prohibit using the identifier cross-border
- Data protection
  - Processing needs to be legitimate
- Liability
  - What if something goes wrong?
- Trust
  - MoUs, Accreditation, self-assessment ??

Project's structure

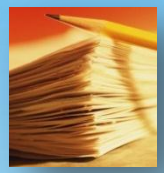


STORK – Roadmap "the way ahead"

Feb 09 | Oct 09 | May10 | May11



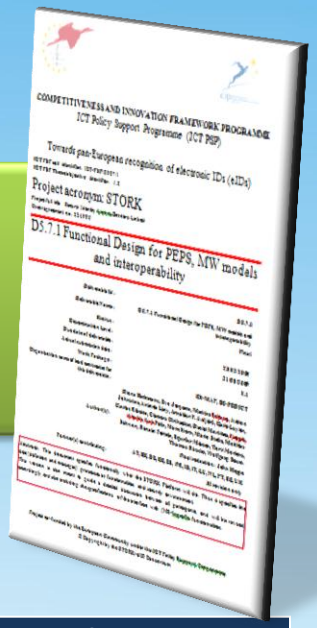
Framework mapping
Legal interoperability
priority technologies



Quality authenticator scheme

eID PROCESS FLOWS

Common, SAML 2.0 - based specifications have been agreed by the STORK consortium



Functional Design

Technical Design

Construction & Implementation

Exploitation - Pilots

Evaluation

Assessment on common specifications on eID

Cross-border authentication platform

Pilots

Pilot 1 – Cross border authentication

Pilot 2 – safer chat

Pilot 3 – eID Student Mobility

Pilot 4 – eID electronic delivery

Pilot 5 – EU Citizen Change of Address

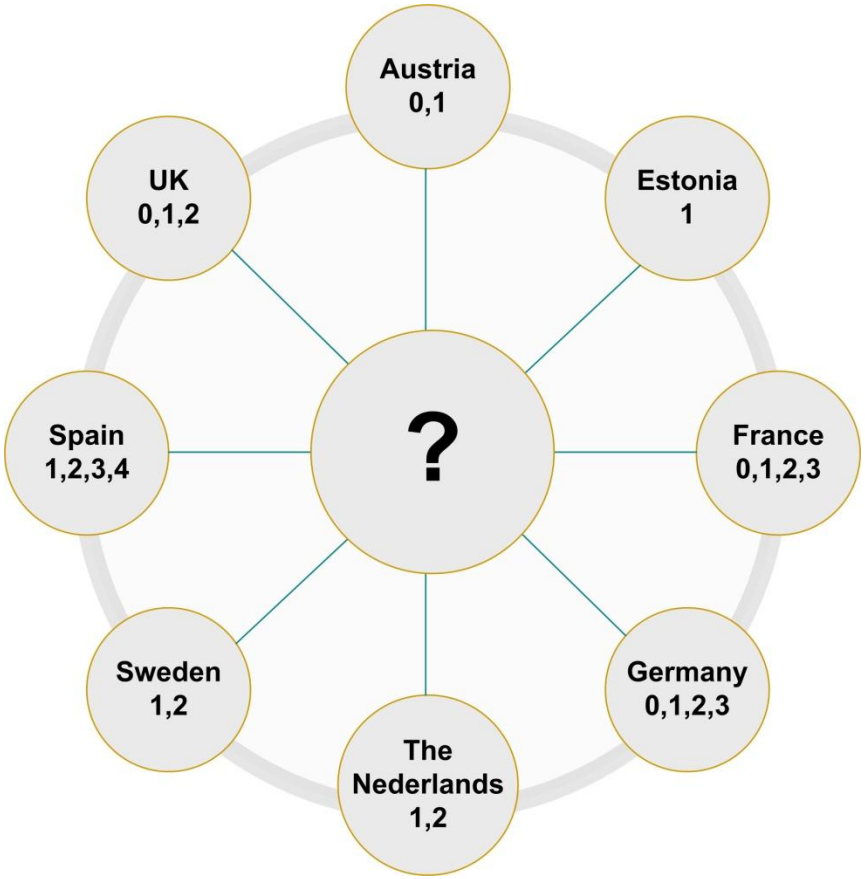
Further services

- A2A services as additional deployments
  - √ Defined as part of the work programme
  - √ First focused on specific applications, but …
- Integration with ECAS
  - √ Obvious option for doing the A2A services with EC
  - √ Demonstrator as a first step
- Establishing as a full STORK pilot (the 6th pilot)

Presentation Overview

- ✓ eID motivation, a little history
- ✓ STORK Project Environment
- Interoperability Models and Integration
- Technology

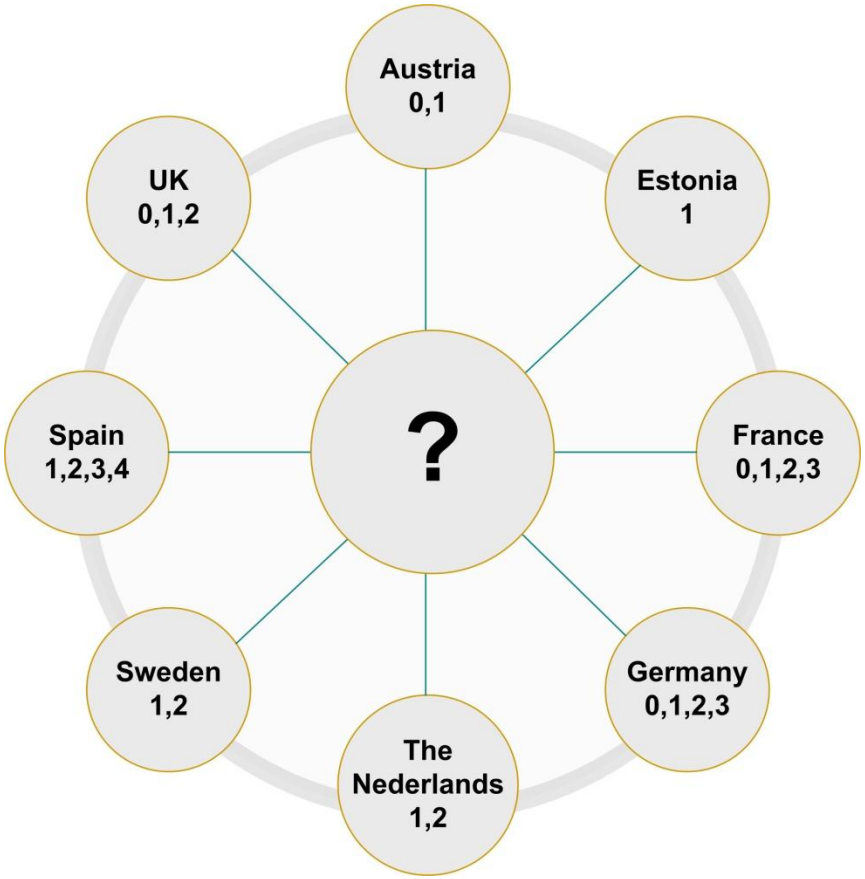
One problem tackled: Trust levels

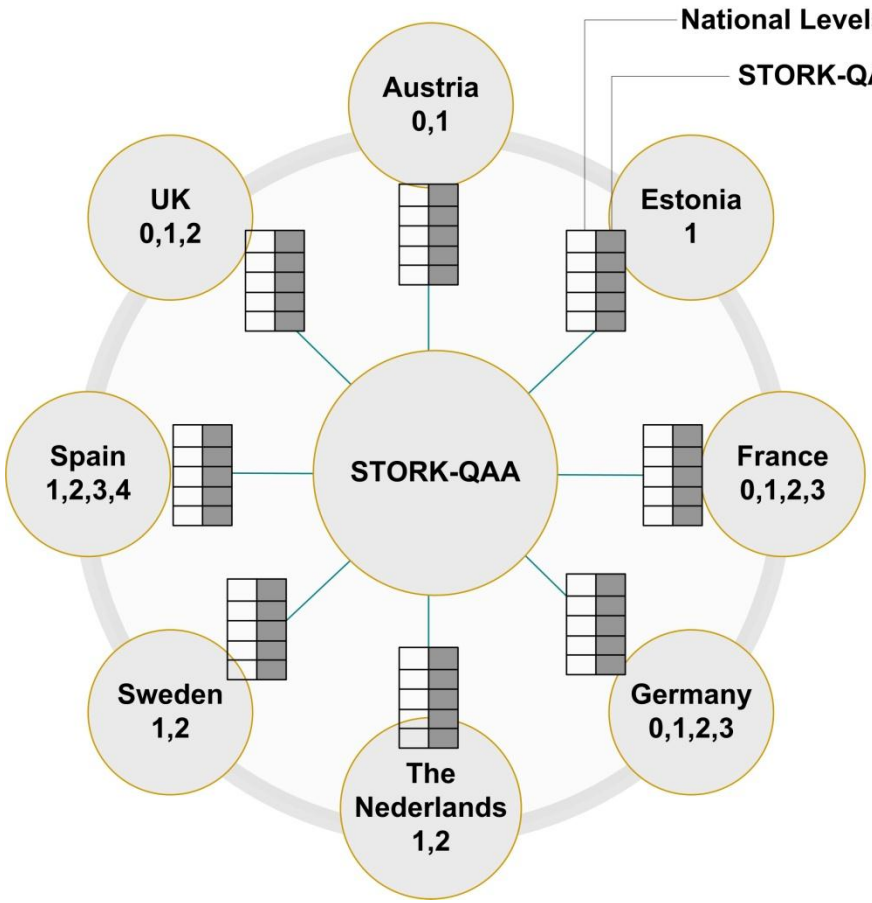


Different technologies and security levels:

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

Approach: Mapping to QAA levels





STORK assumes the citizen has online-access with eID.

Four use cases:

1. **Authentication:** in an online access to a service provider
2. **Attribute Transfer**
   - STORK defines ***eID*** as the ***identifier*** (e.g. national citizen ID),
   - "the rest" (name, date of birth, qualification, …) are ***attributes***
3. **Attribute Verification:** is a certain attribute presented by the citizen correct?
4. **Certificate Verification:** for electronic signatures

One Interoperability Framework, Two Basic Models

STORK will investigate and pilot two interoperability models:

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

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

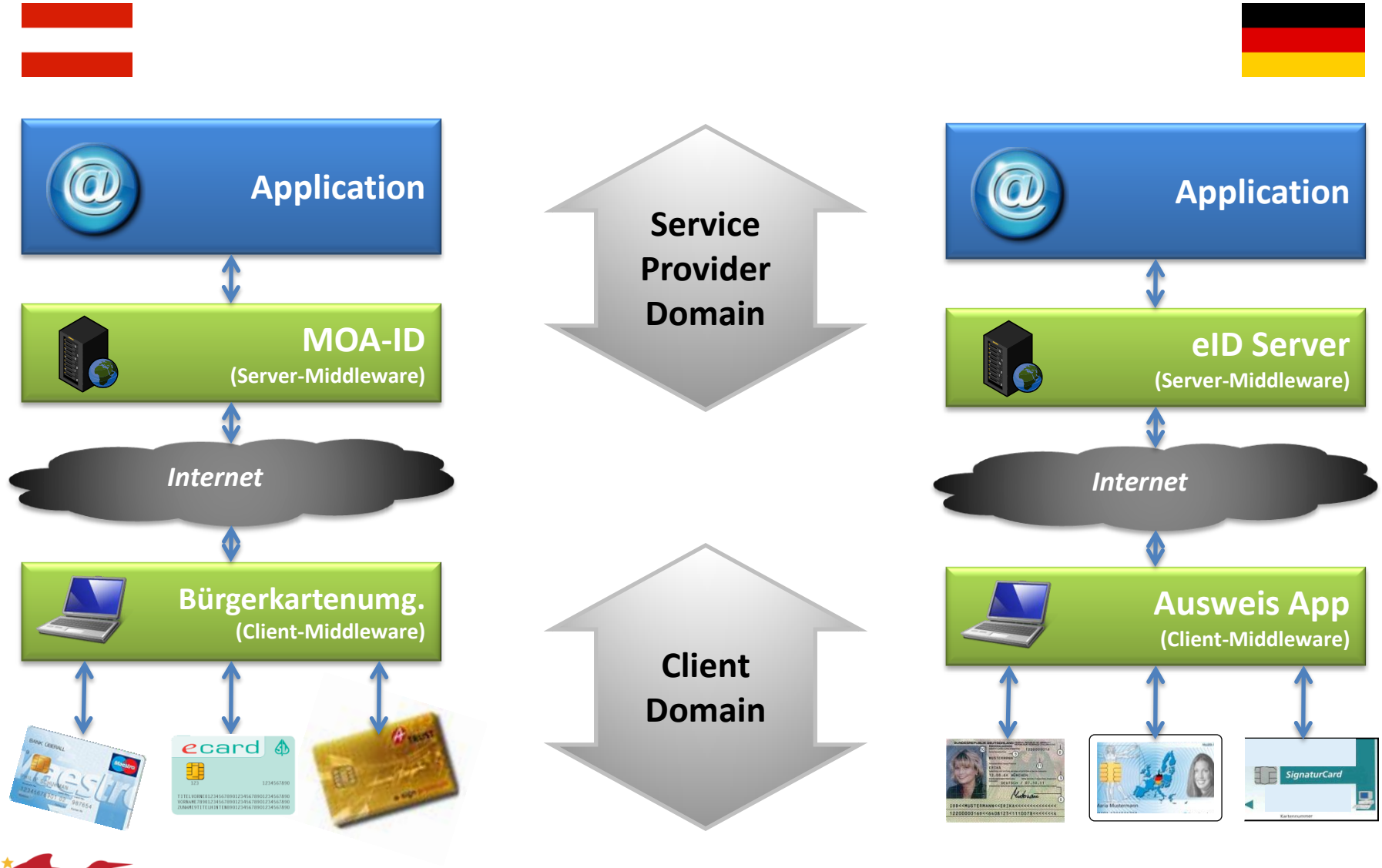
The common specifications have been designed so that major components operate on the same protocols, irrespective of the model or its combinations.

STORK – High Level Architectural Approach 1

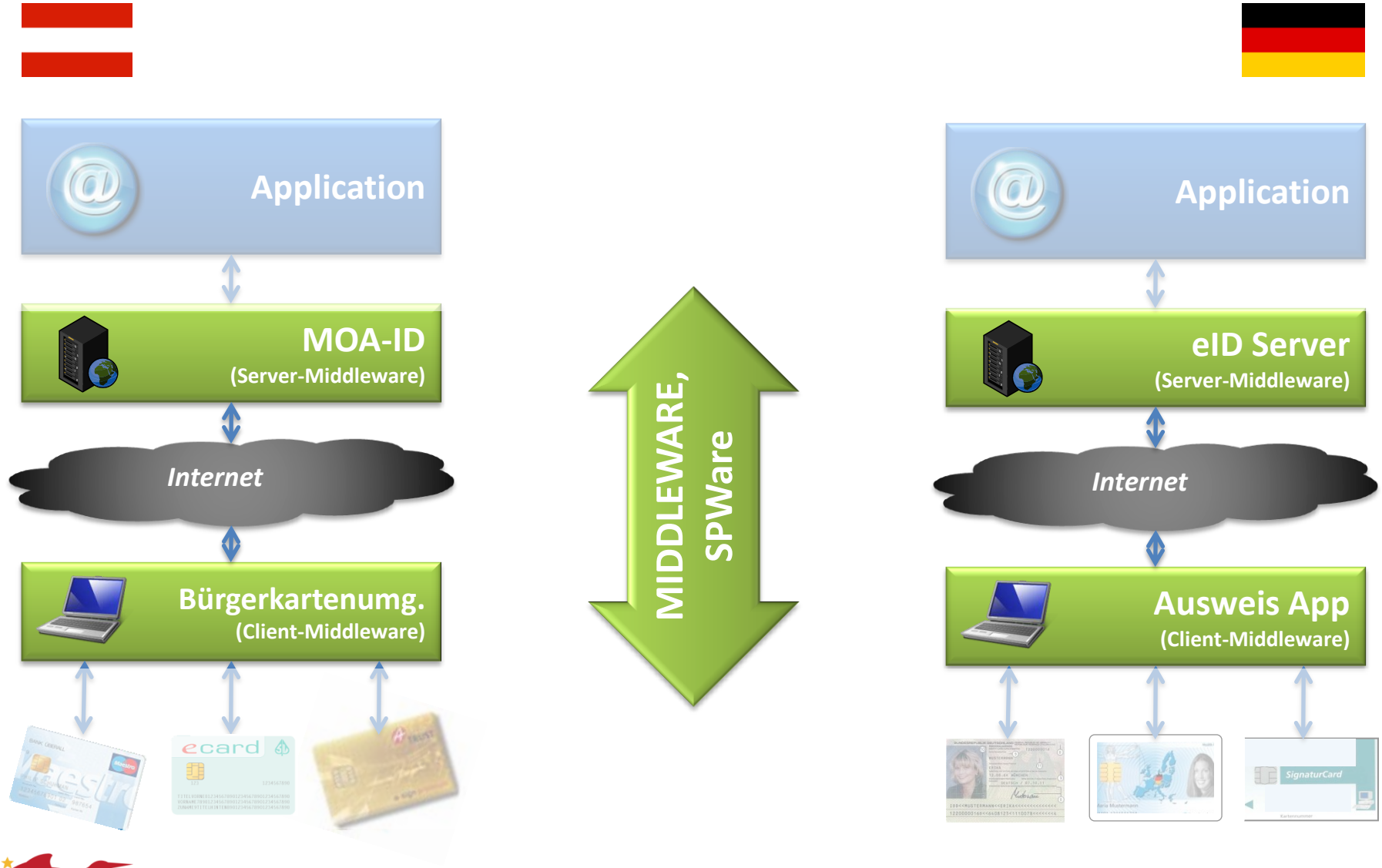
Integration at the Service Provider with smart-cards as means of eID

Middleware

STORK – Example of Middleware Architectures

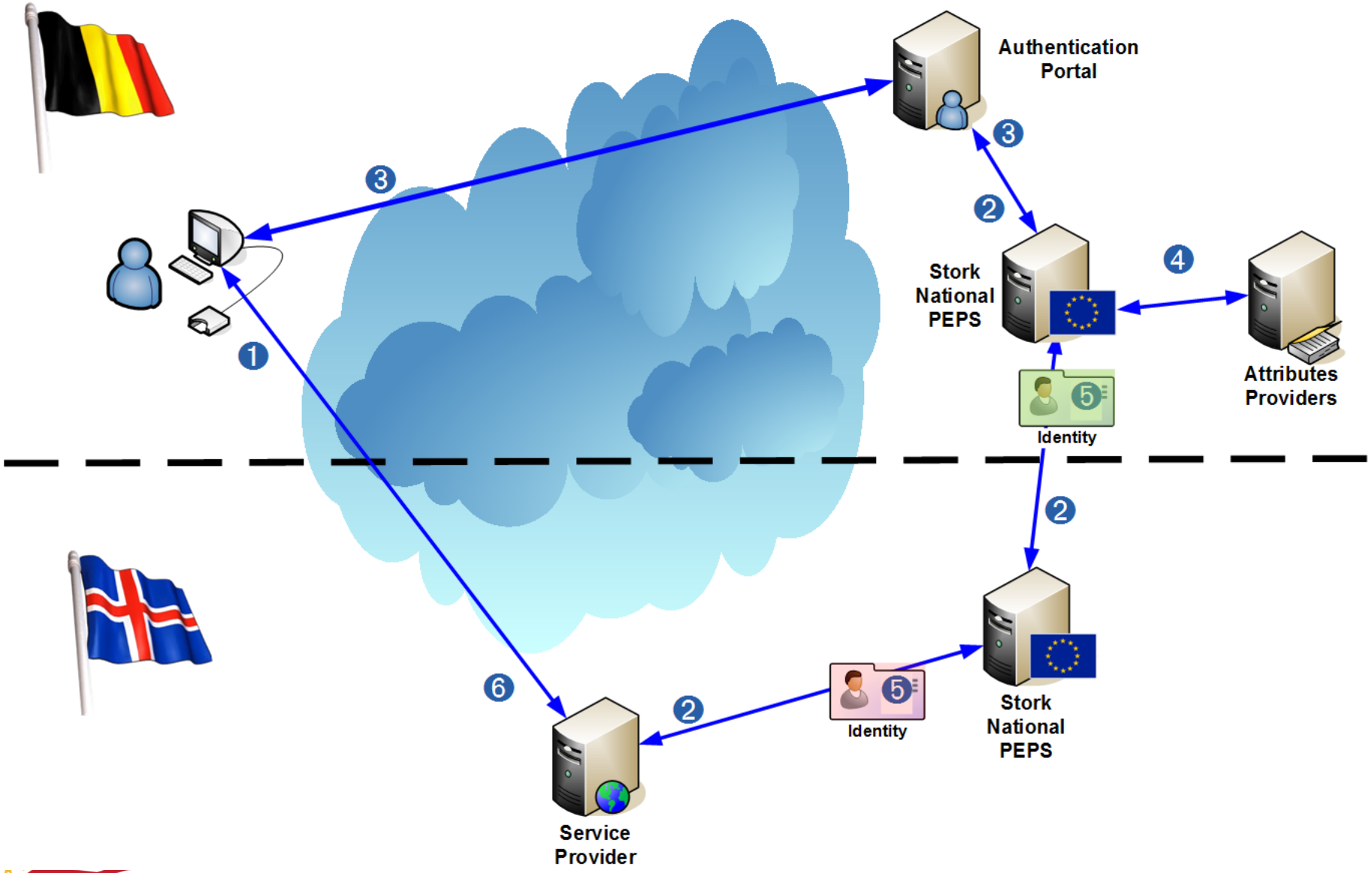


STORK – Communalities: Middleware Concept

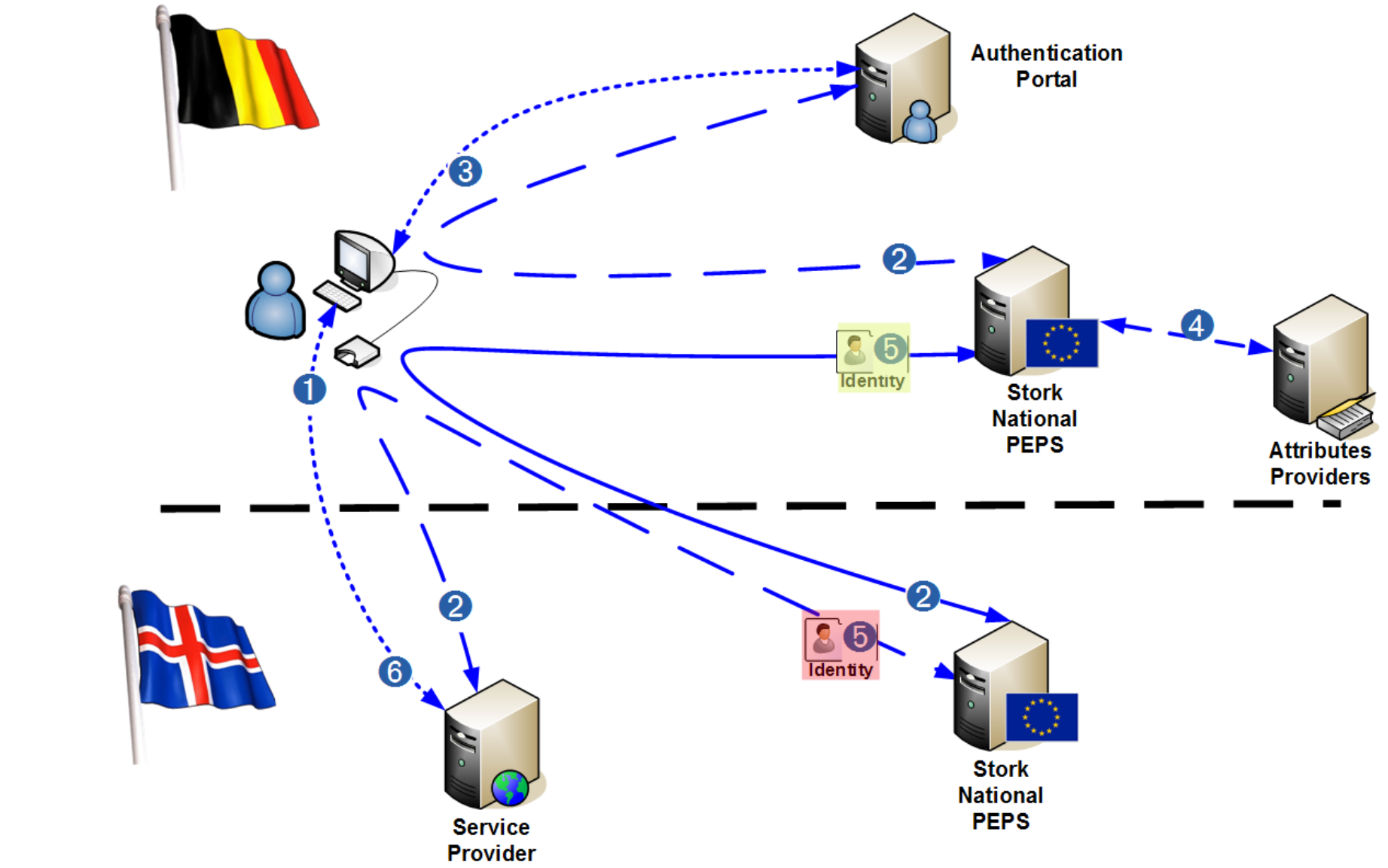


STORK – Making Governments to co-operate

STORK PEPS data flow (logical)



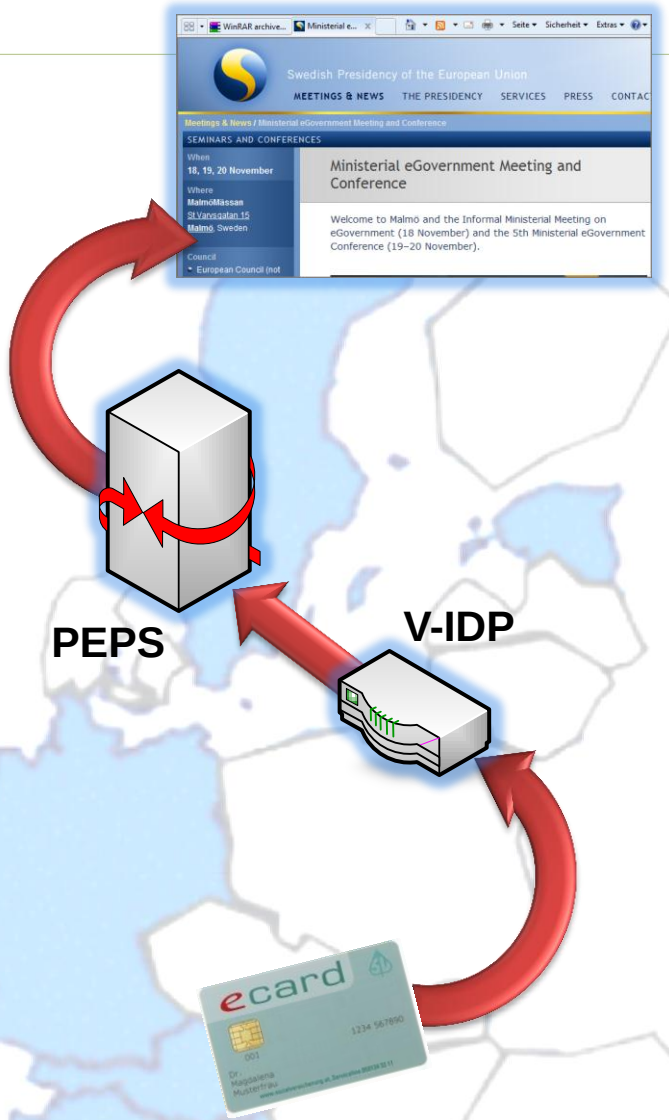
Protocol: Federated Identity (SAML 2.0)



The “combination hat trick” V-IDP

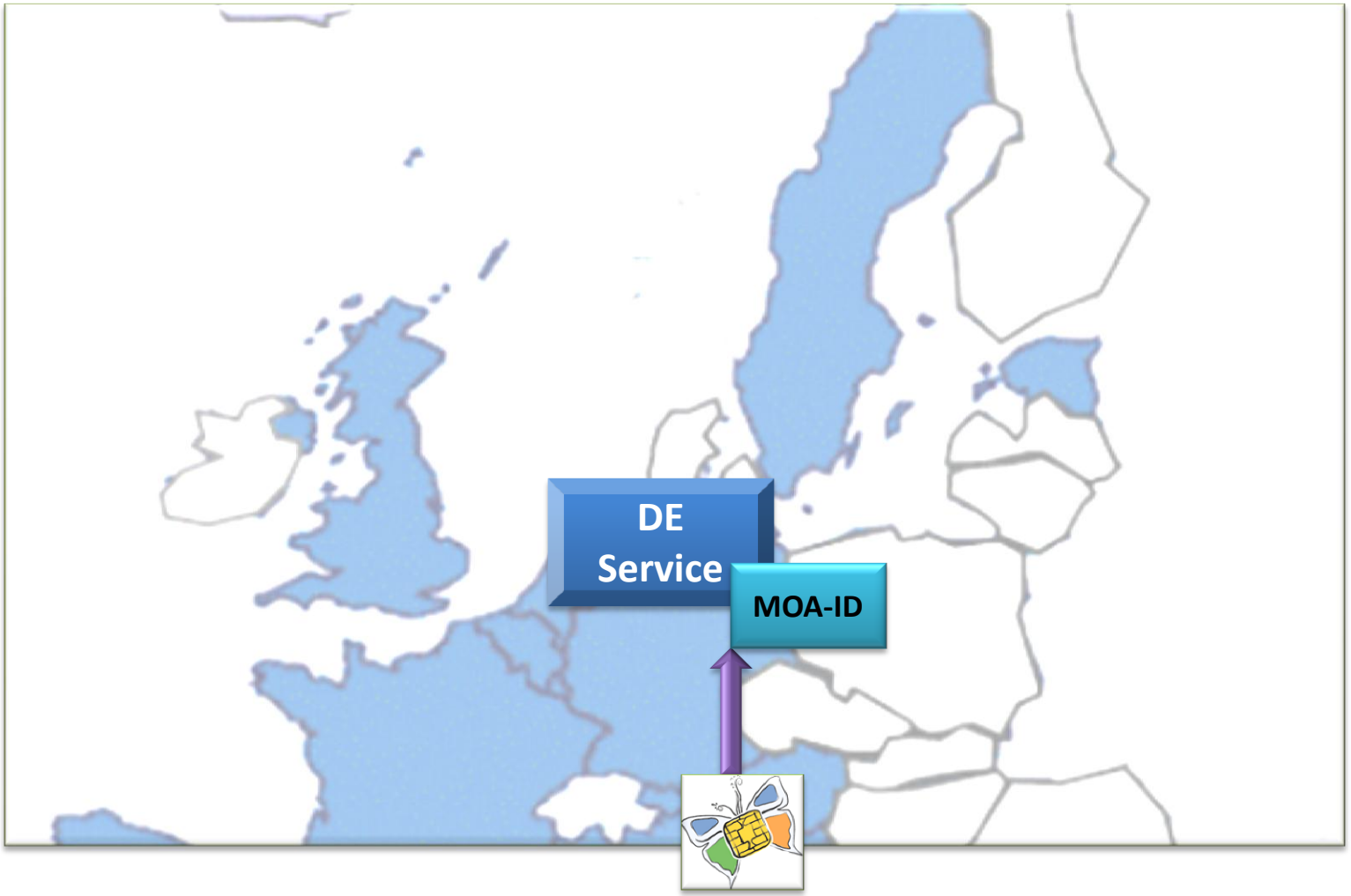
Virtual Identity Provider

- provide a MW access at a PEPS or
- a PEPS interface at the SPware



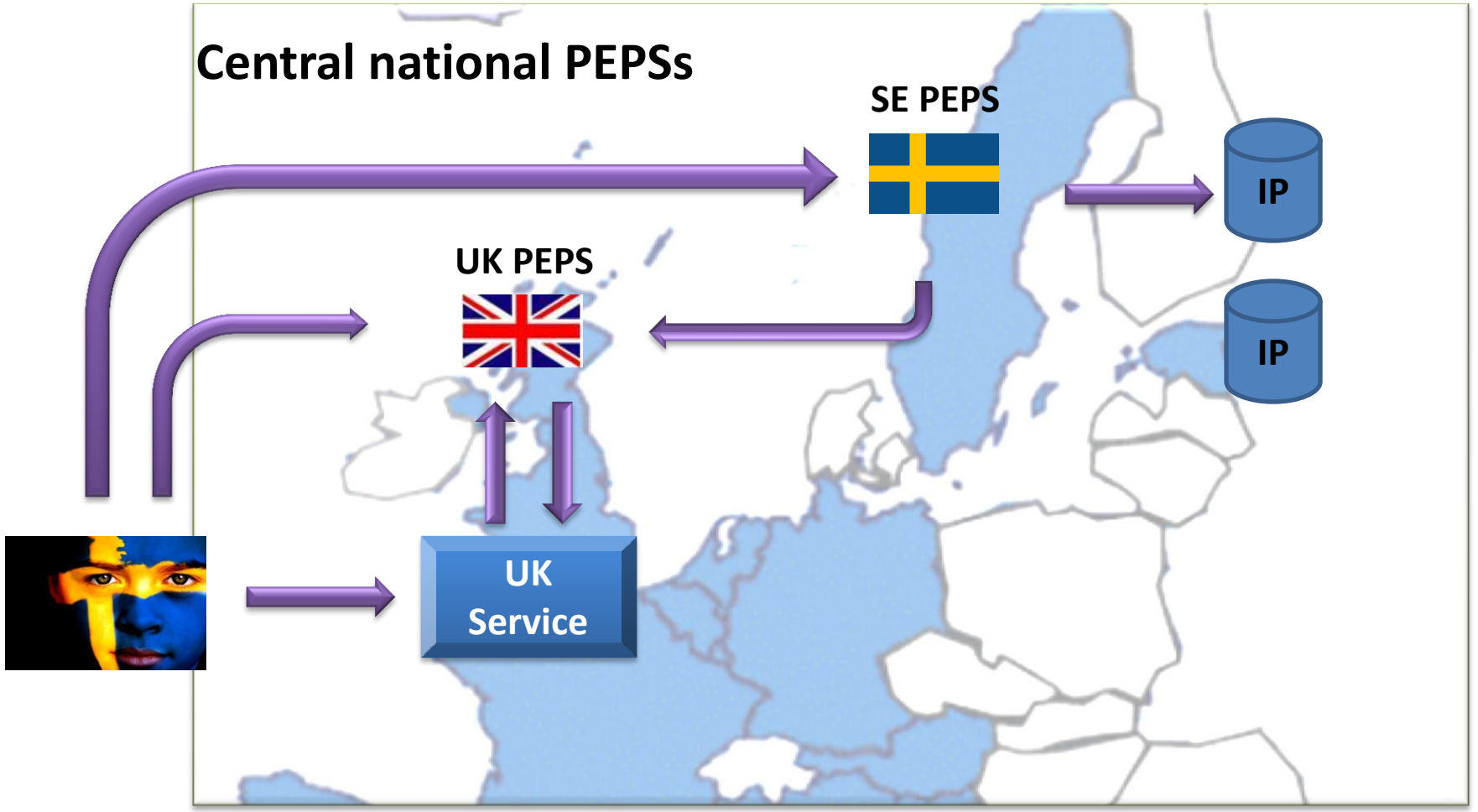
STORK – Middleware Interoperability Model

MW ⇨ MW example: Austrian student at German University



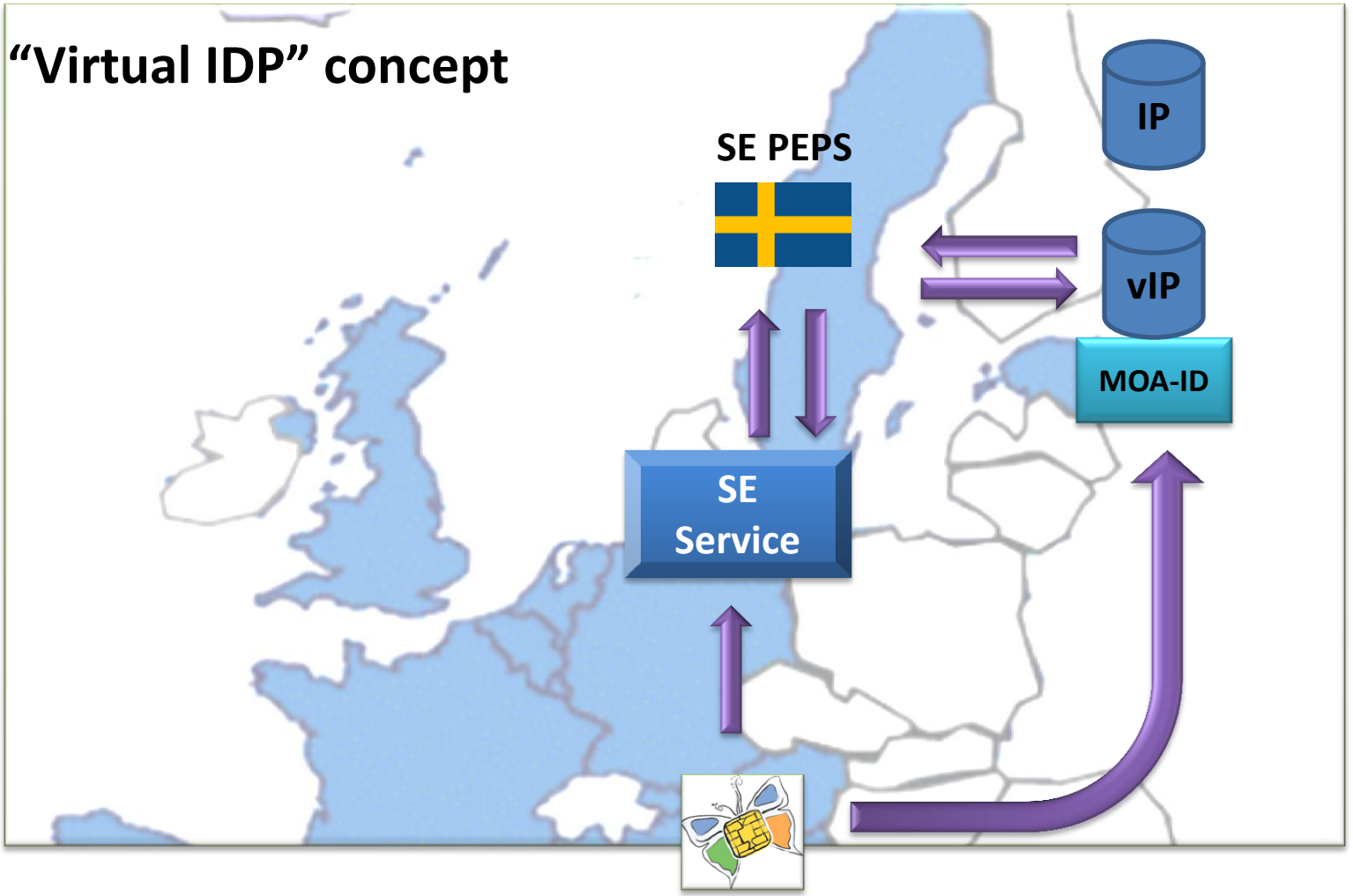
STORK – PEPS Interoperability Model

PEPS example: Swedish student at UK university



STORK – combined model

MW ⇨ PEPS example: Austrian student at Swedish university,

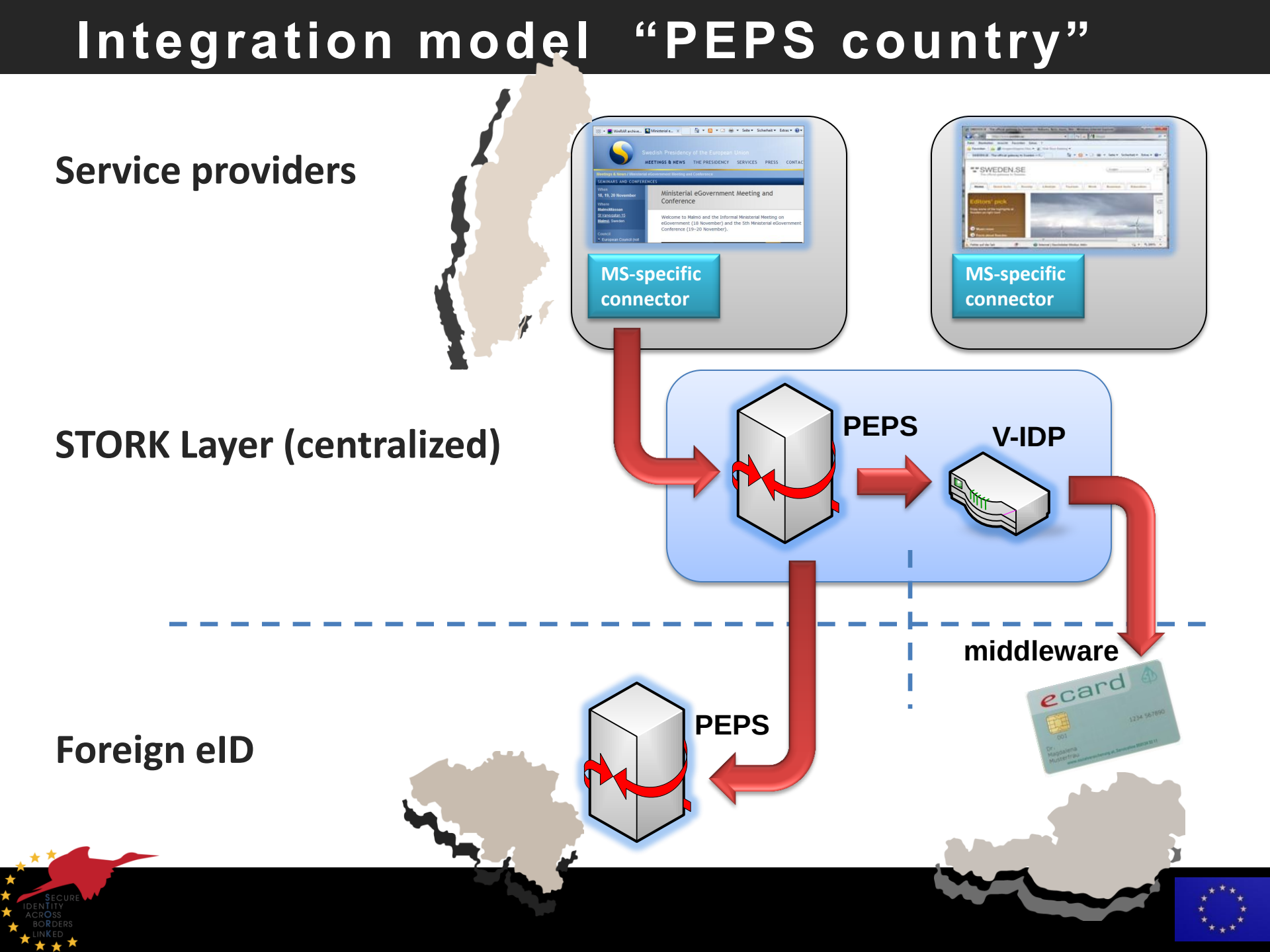


General considerations

- 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

Integration model "PEPS country"



Integration model "MW country"

Service providers

STORK Layer (decentralized)

Foreign eID

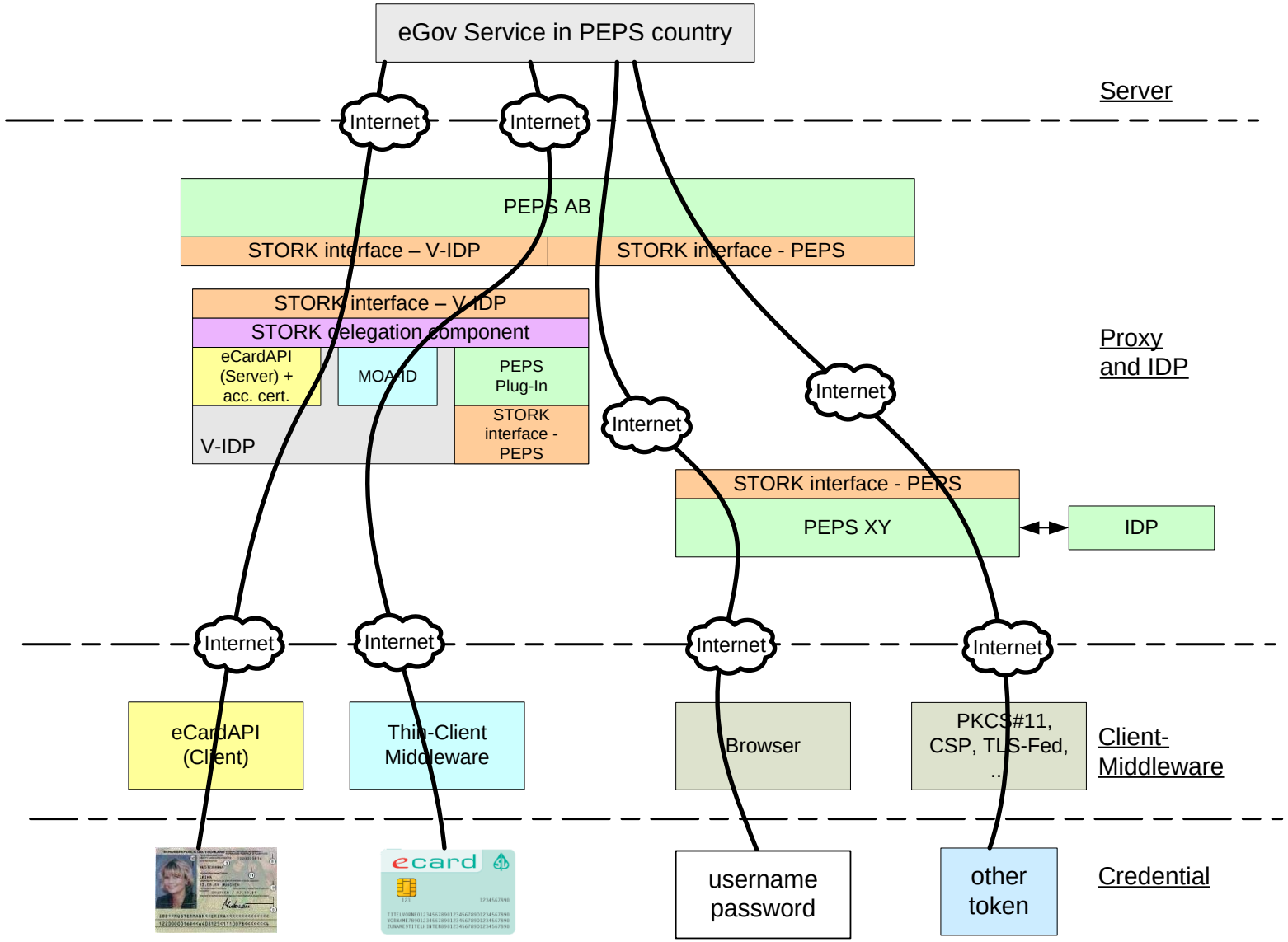
middleware

PEPS

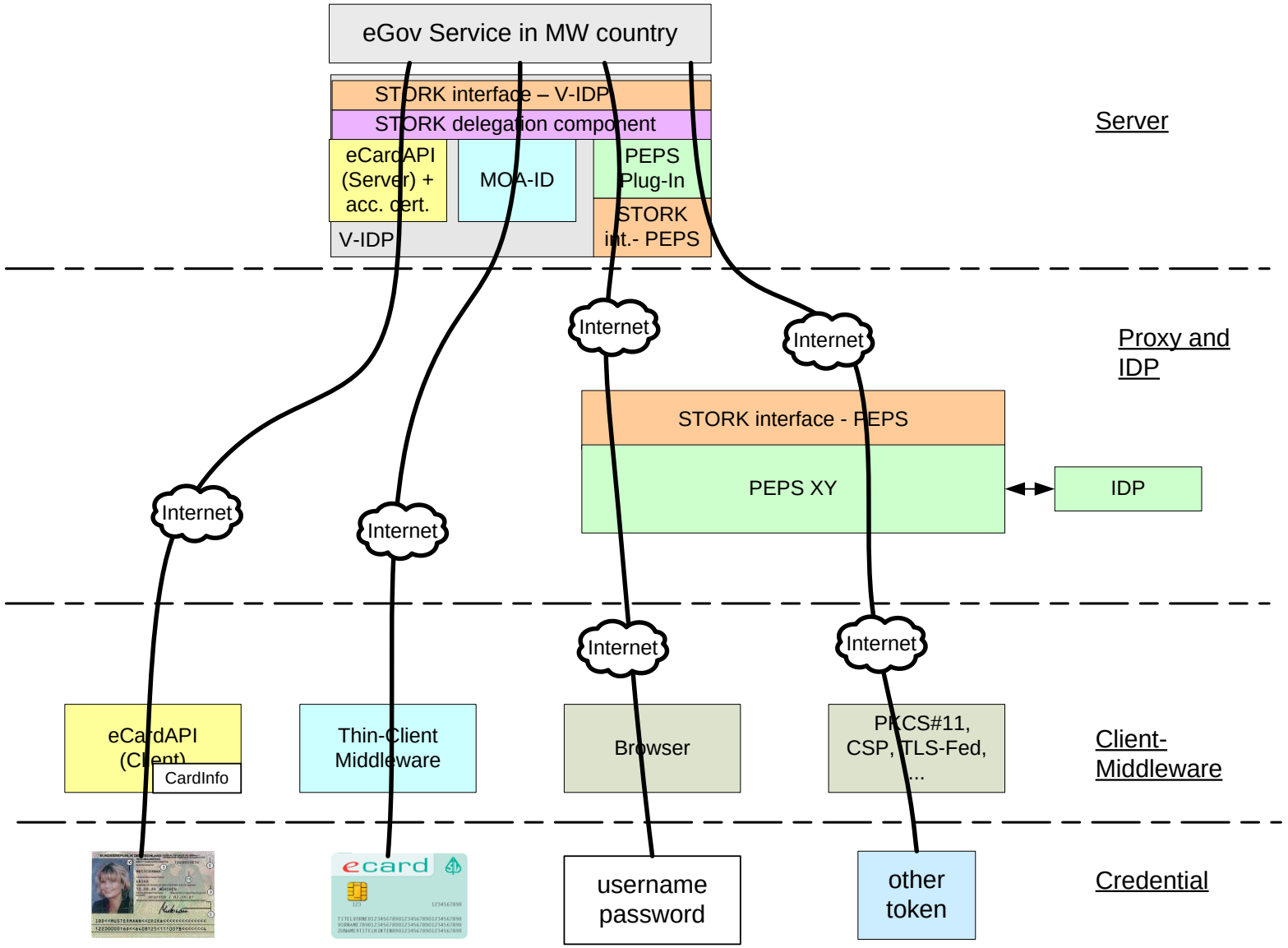
Presentation Overview

- ✓ eID motivation, a little history
- ✓ STORK Project Environment
- ✓ Interoperability Models and Integration
- Technology

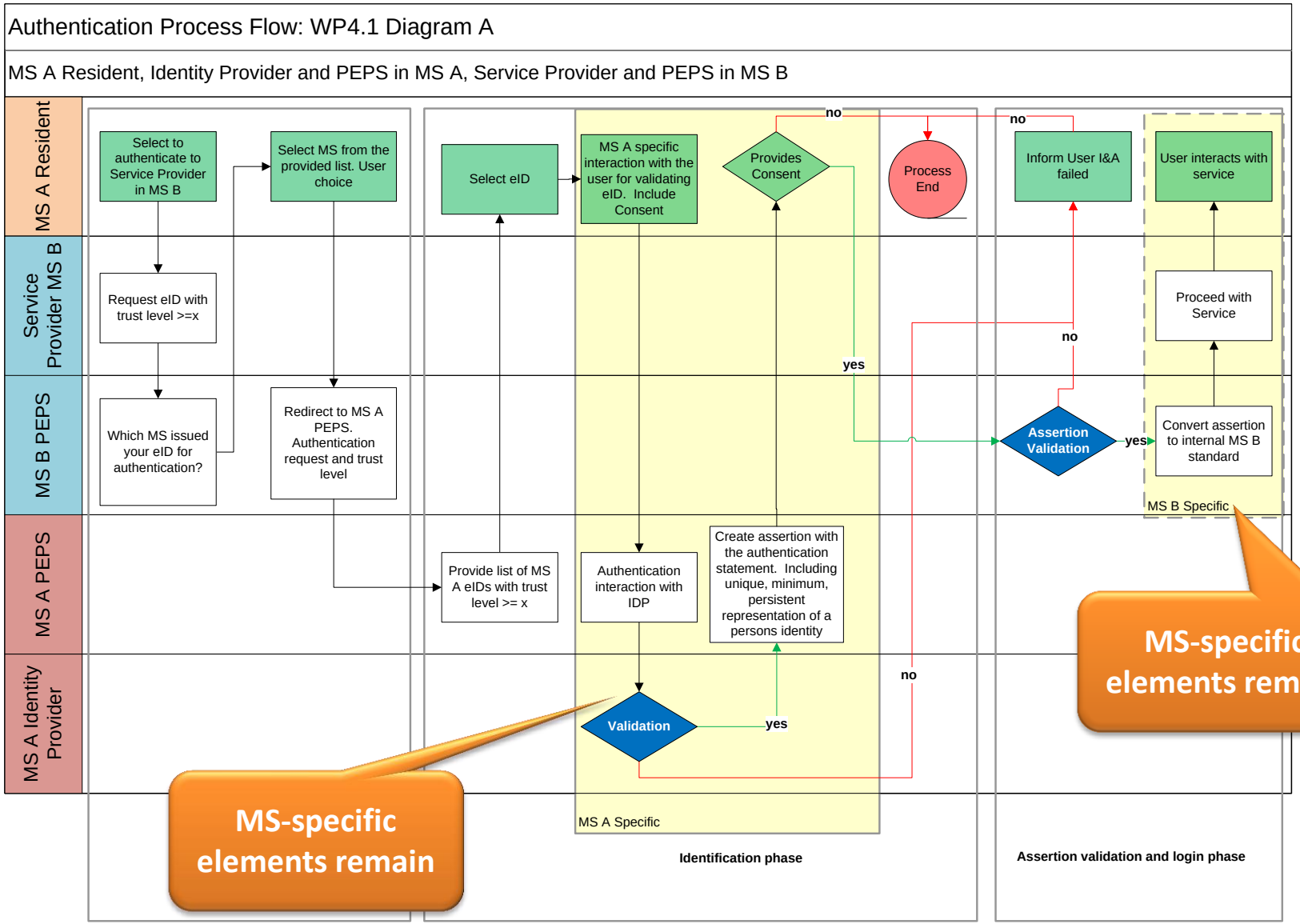
Case 1: Service Provider in PEPS State



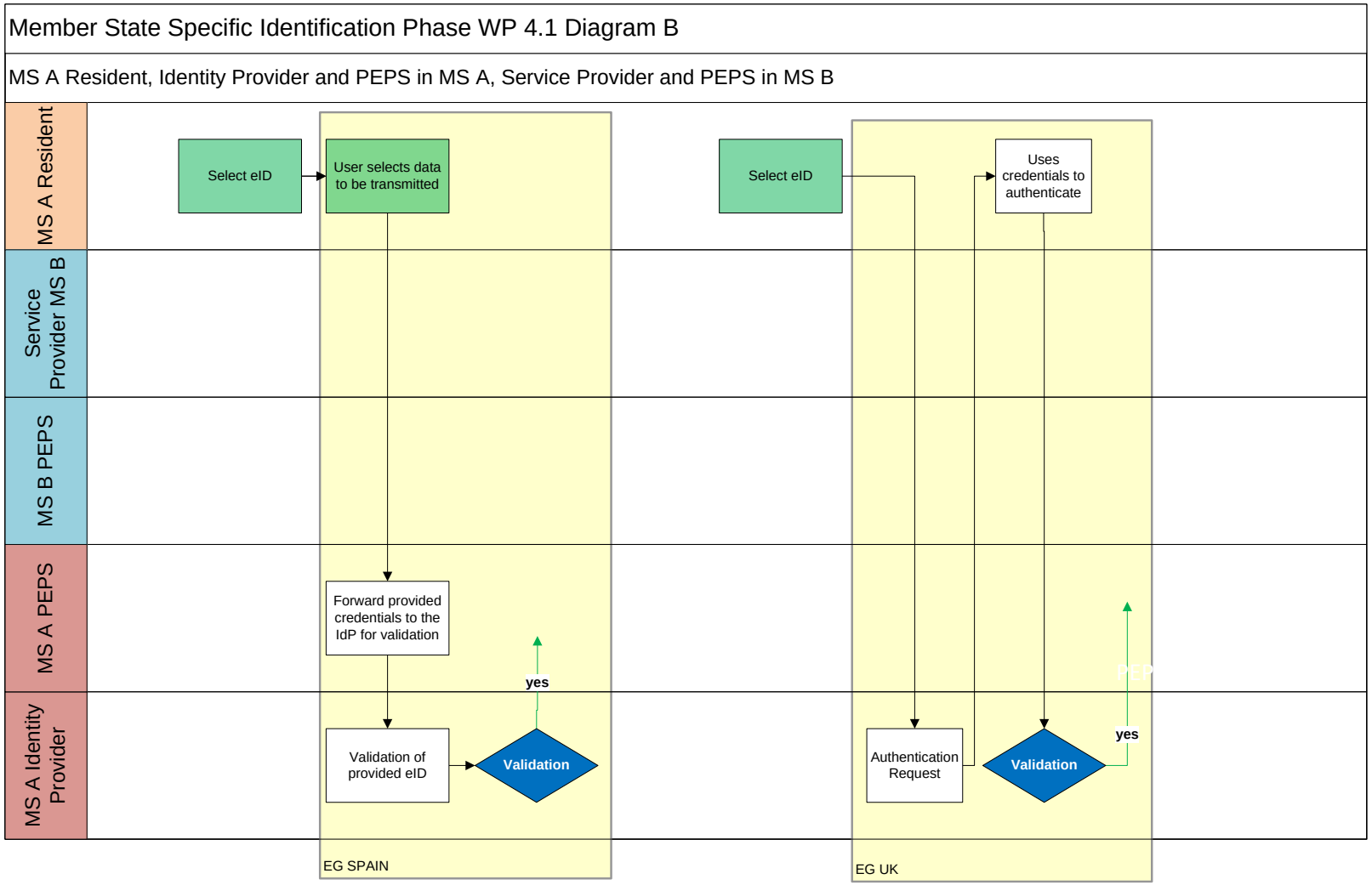
Case 2: Service Provider in MW State



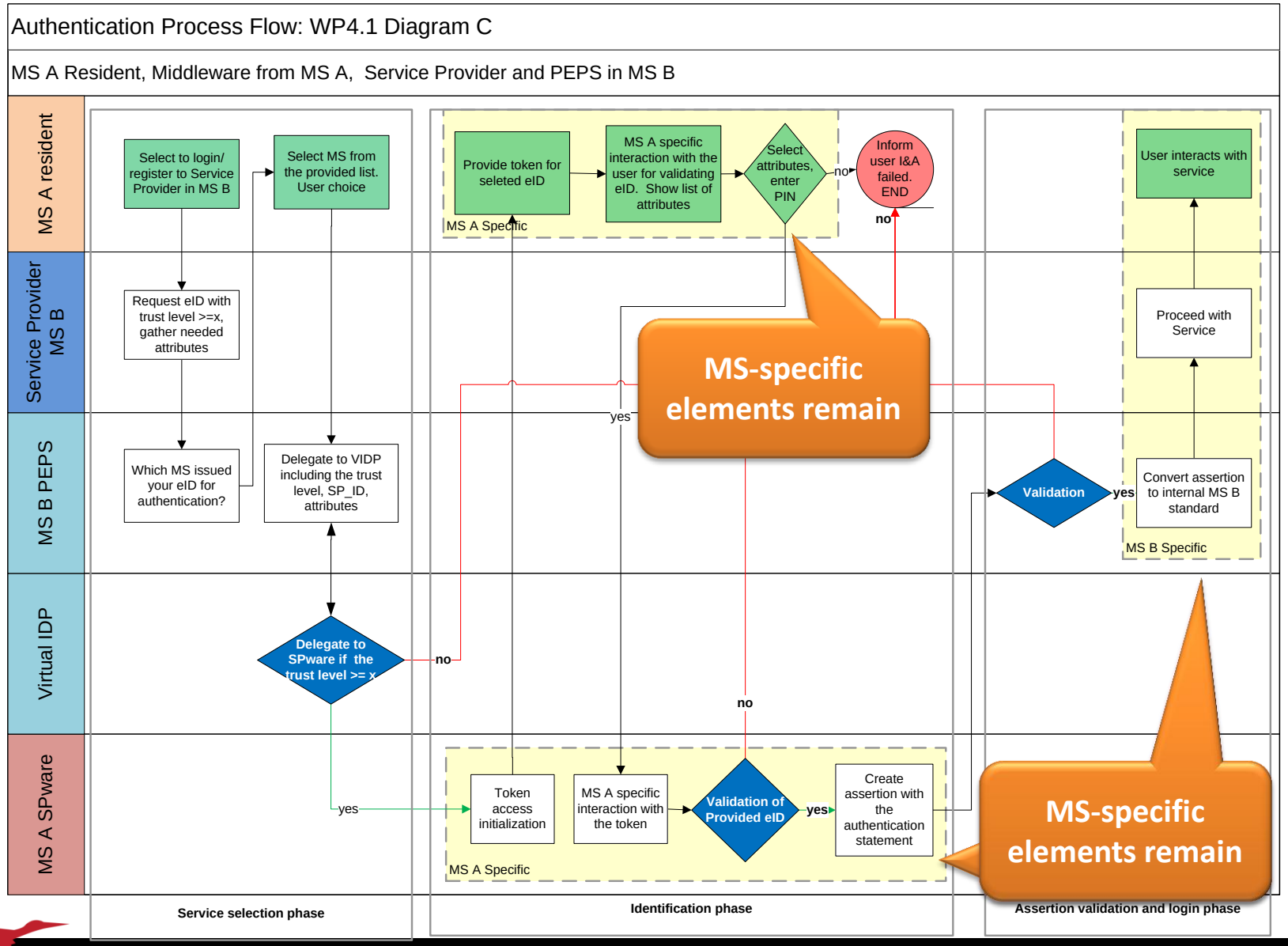
STORK – Process Flow PEPS-PEPS Authentication



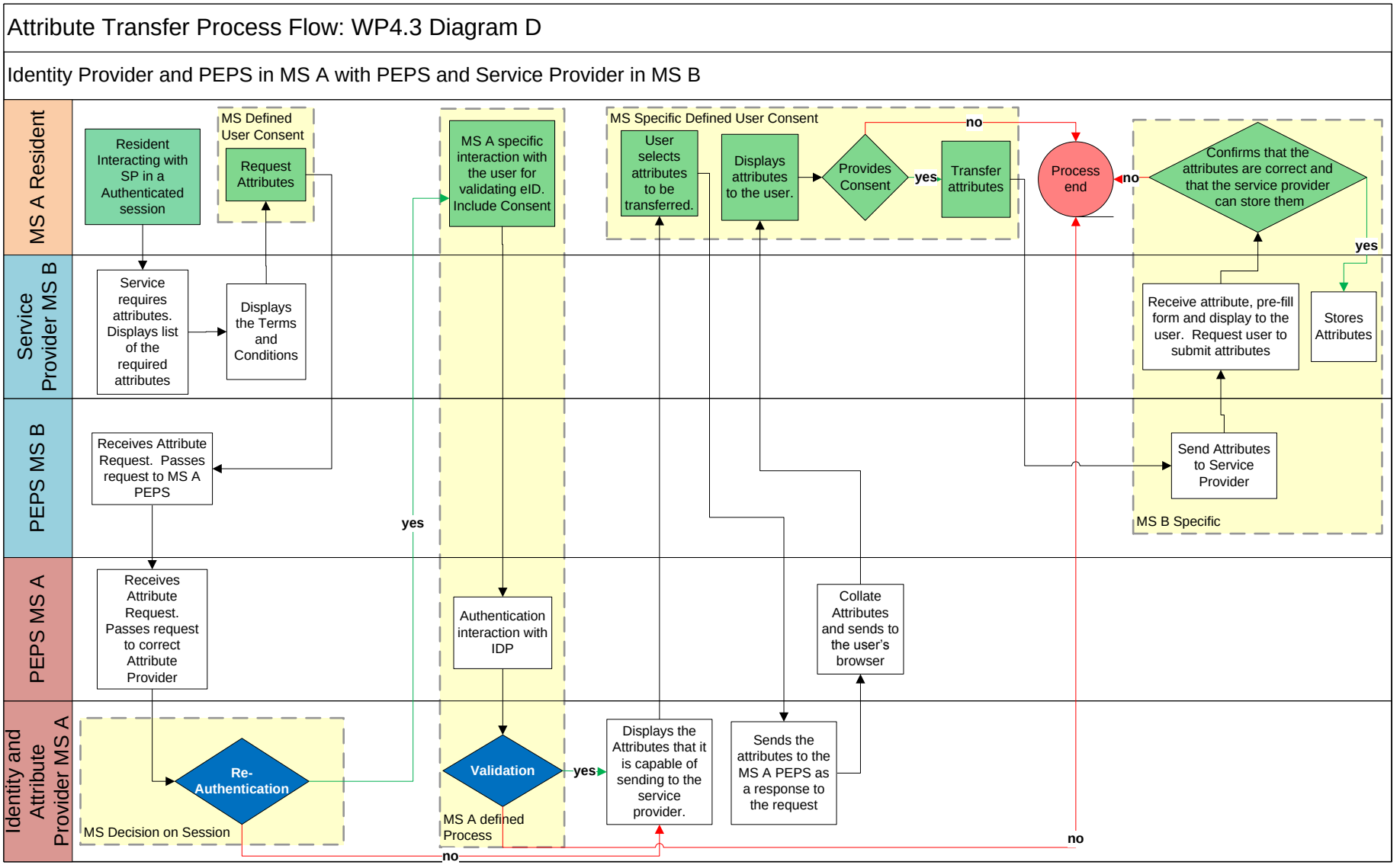
STORK – Process Flow PEPS-PEPS MS-specific



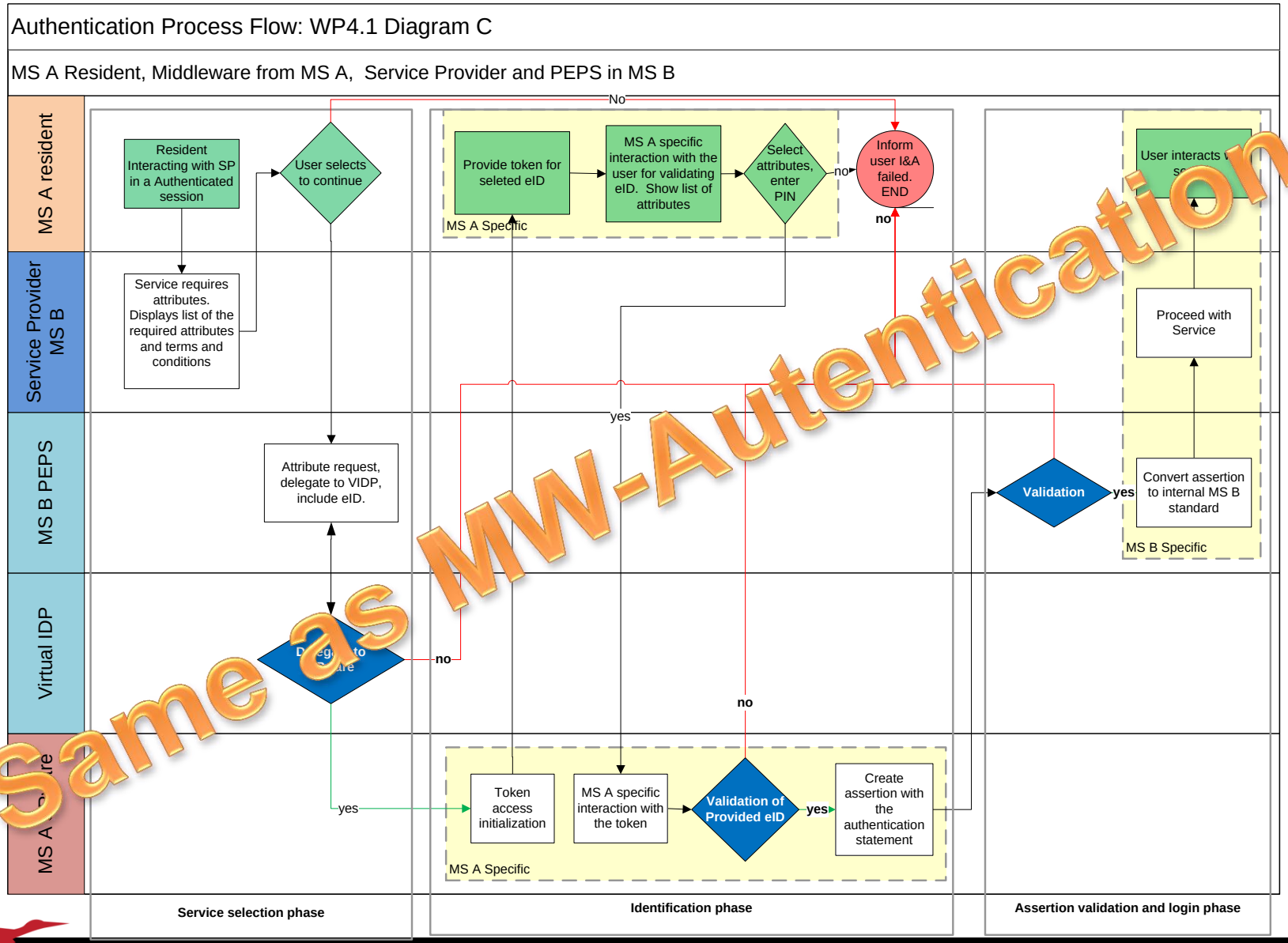
STORK – Process Flow MW-PEPS Authentication



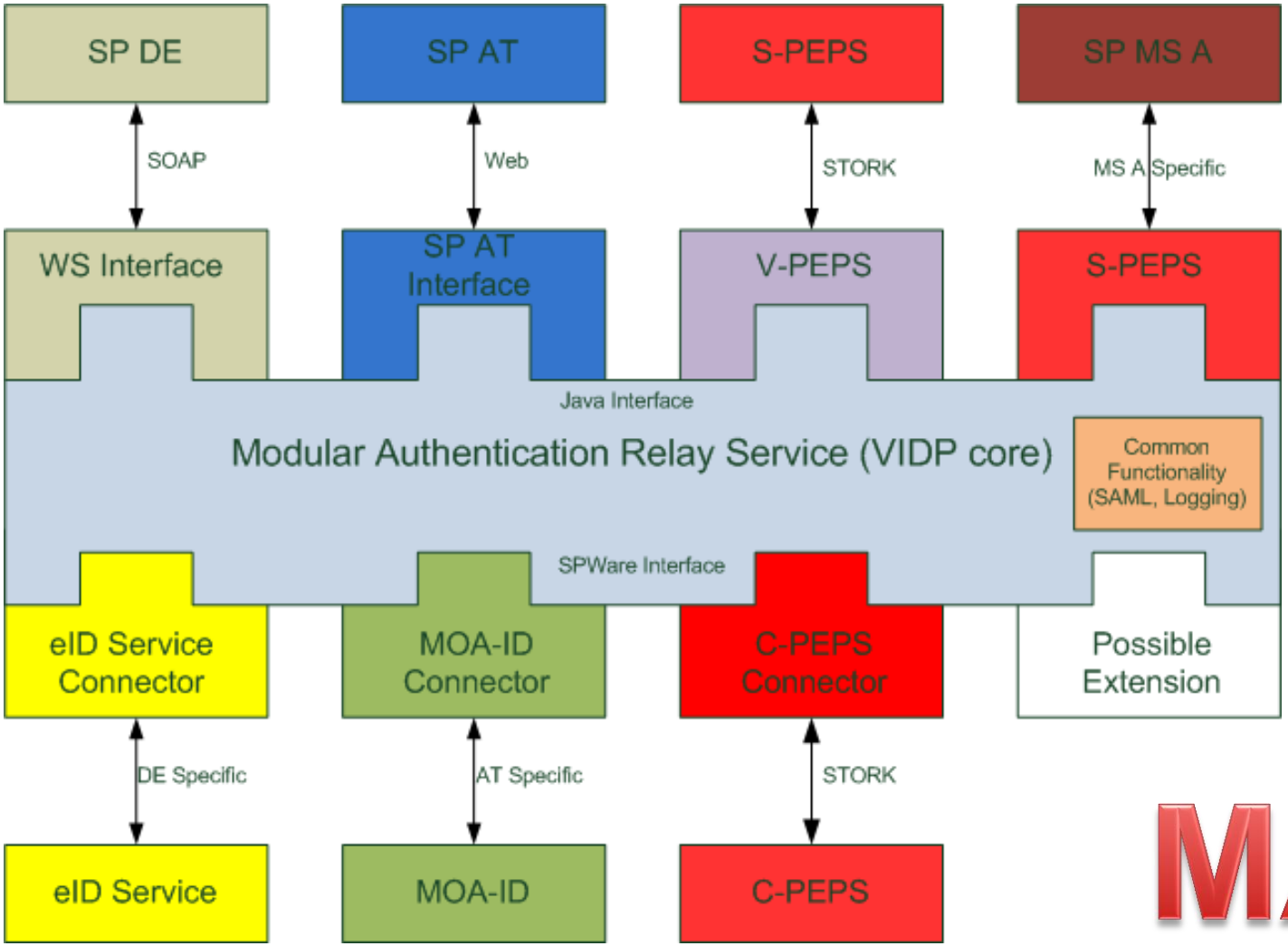
STORK – Process Flow PEPS Attribute Transfer



STORK – Process Flow MW-PEPS Attribute Transf.

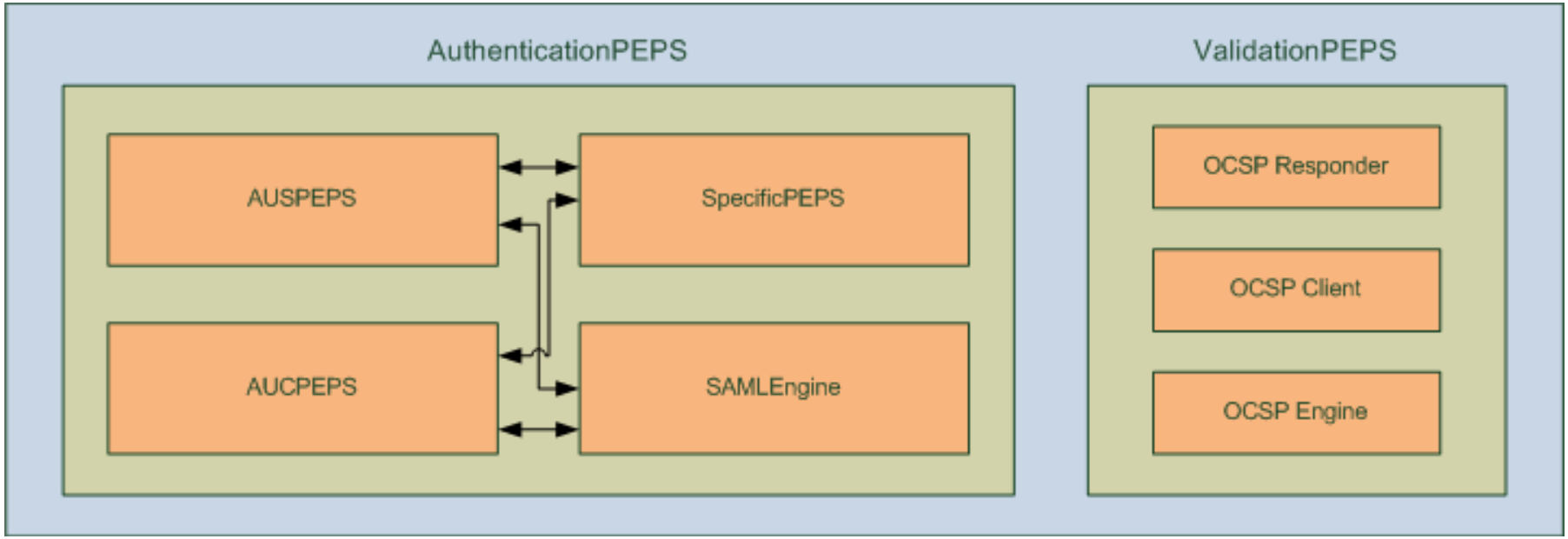


Common MW architecture



MARS

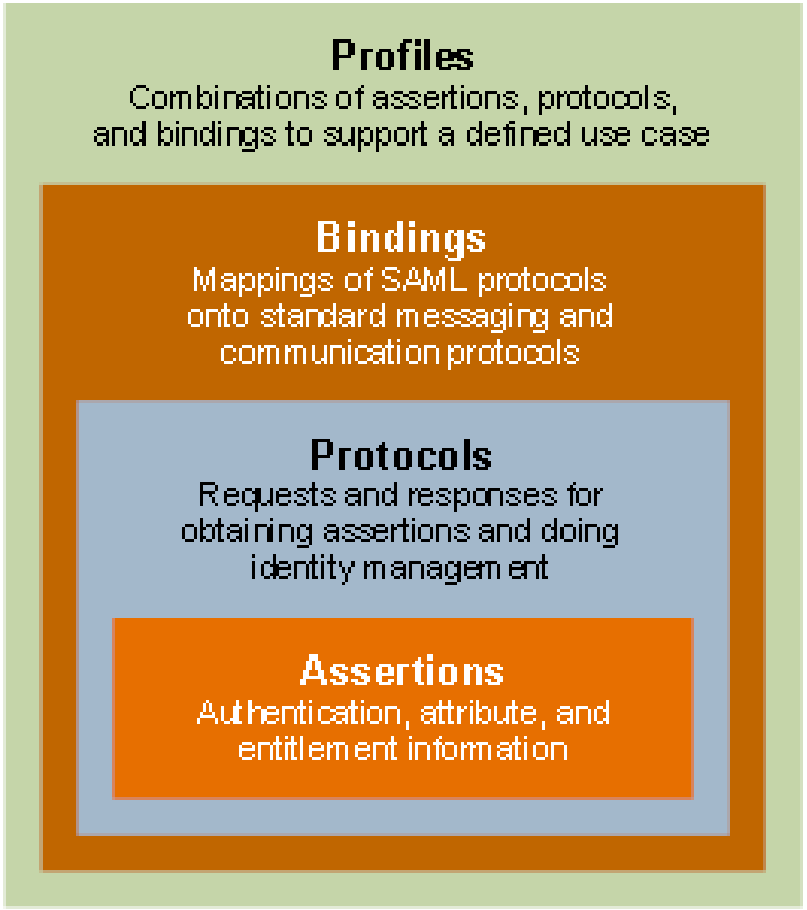
PEPS Architecture



Security Assertion Markup Language (SAML)

- XML-based standard for exchanging authentication and authorization data between security domains
- Typical Use Cases:
  - √ Web Single Sign-On (SSO)
  - √ Identity Federation
  - √ Attribute-Based Authorization
  - √ Securing Web Services

SAML architecture



SSO Profiles, Single Logout Profile, Attribute Profiles, …

SOAP Binding, HTTP- Artifact, HTTP-Redirect, HTTP-Post Binding, …

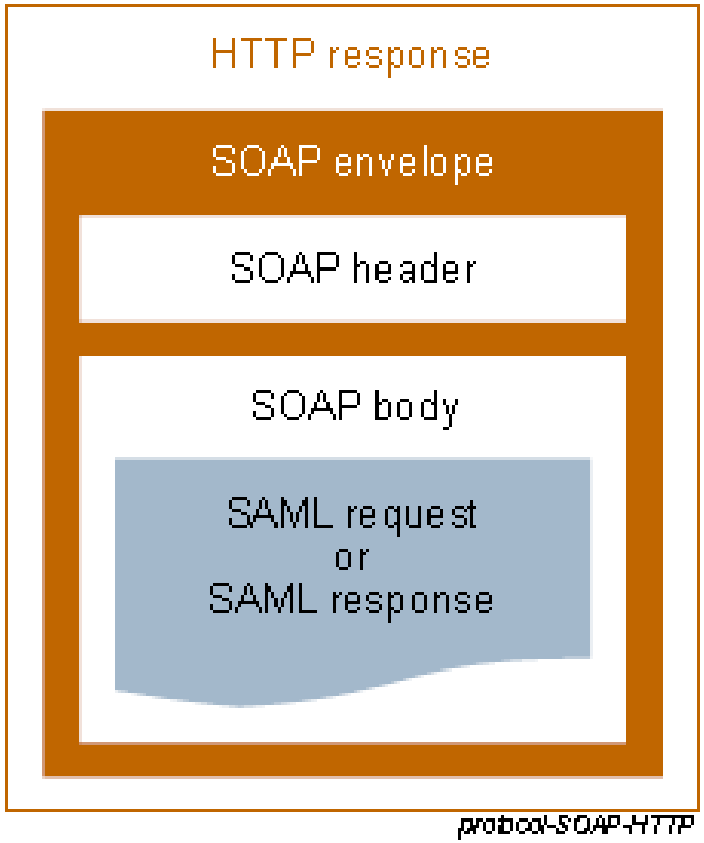
Authentication Request Protocol, Single Logout Protocol, …

Authentication, Attribute, Authorization Decision Assertion

Source: SAML 2.0 Technical Overview

SAML example

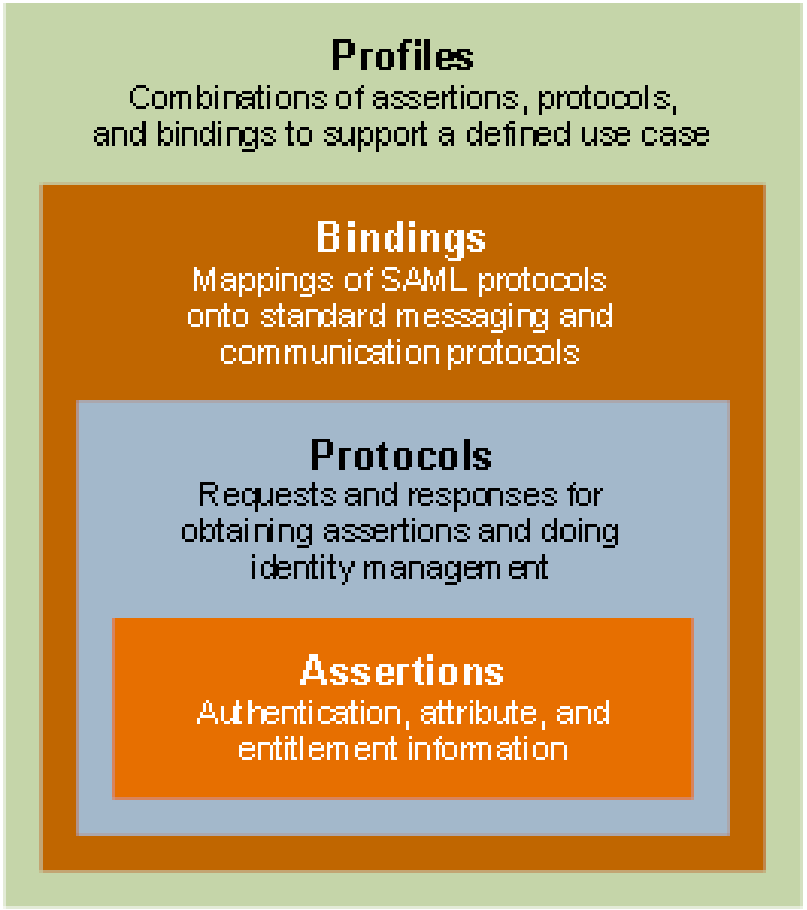
- SAML via SOAP over HTTP




```
 1: <?xml version="1.0" encoding="UTF-8"?>
 2: <env:Envelope  xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 3:   <env:Body>
 4:     <samlp:Response
 5:       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 6:       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 7:       Version="2.0"
 8:       ID="i92f8b5230dc04d73e93095719d191915fdc67d5e"
 9:       IssueInstant="2006-07-17T20:31:41Z"
10:       InResponseTo="aaf23196-1773-2113-474a-fe114412ab72 ">
11:       <saml:Issuer>http://idp.example.org</saml:Issuer>
12:       <samlp:Status>
13:         <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
14:       </samlp:Status>
15:                     ...SAML assertion...
16:     </samlp:Response>
17:   </env:Body>
18: </env:Envelope>
```

Source: SAML 2.0 Technical Overview

SAML and STORK



Web Browser SSO Profile, Holder of Key Web Browser SSO Profile

HTTP-Post Binding, SOAP Binding

Authentication Request Protocol (amended to include Attribute Query)

Authentication and Attribute Assertion

PEPS – Environment and Frameworks

- Linux/Windows
- Java 1.5
- Application Servers – Web application
  - √ Tomcat 5/6
  - √ JBoss 5
  - √ Glassfish V3
- Frameworks:
  - √ Spring
  - √ Struts
  - √ OpenSAML
  - √ log4j

VIDP – Environment and Frameworks

- Linux/Windows
- Java 1.5
- Application Servers – Enterprise application
  - √ Glassfish V2
- Frameworks:
  - √ EJB
  - √ Velocity (Web presentation, JSP)
  - √ OpenSAML
  - √ slf4j/log4j
  - √ JAXB/JAX-WS

Presentation Overview

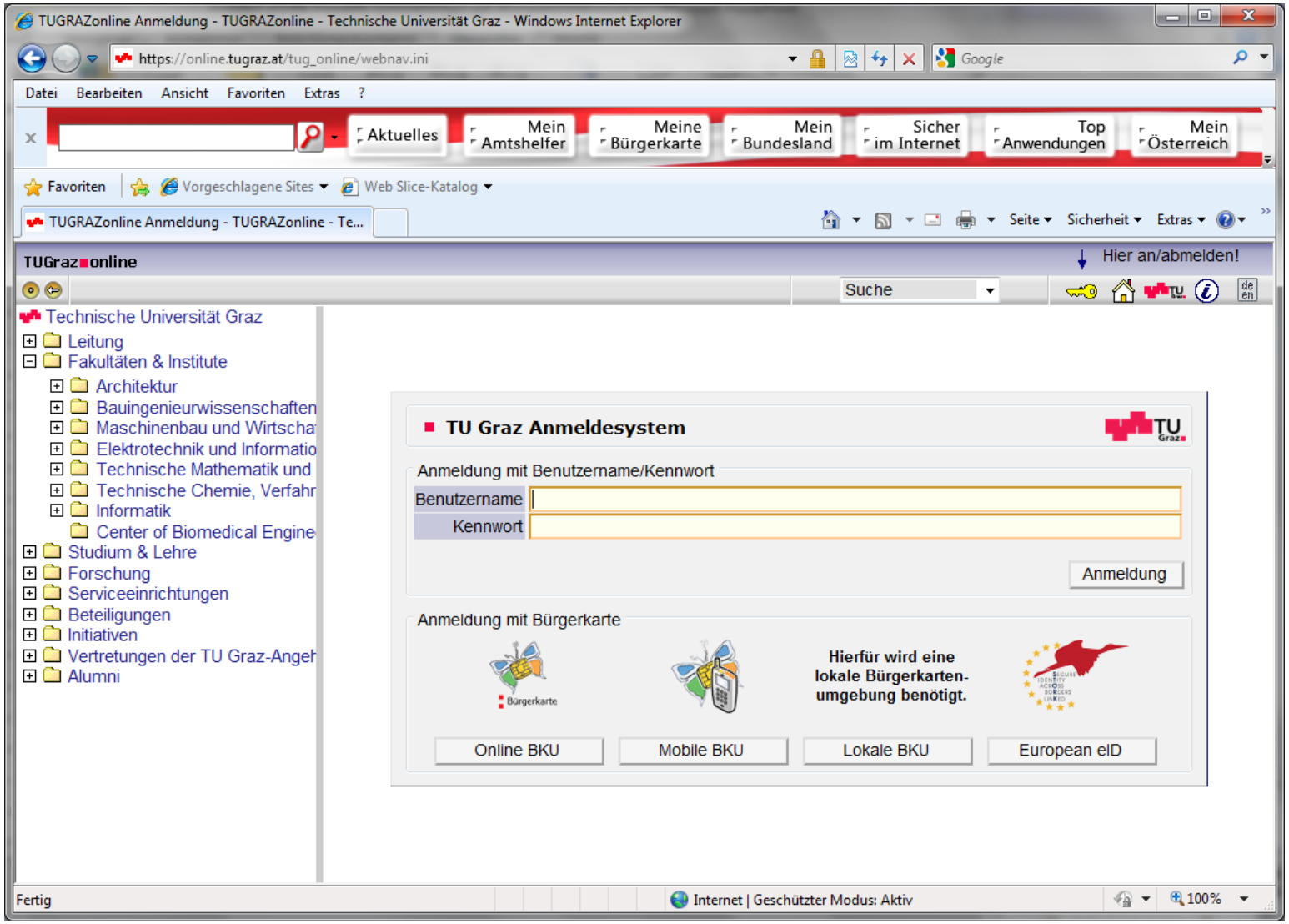
- ✓ eID motivation, a little history
- ✓ STORK Project Environment
- ✓ Interoperability Models and Integration
- ✓ Technology

Next step: Digital Agenda (May 2010)

Key Action 3: In 2011 propose a revision of the **eSignature Directive** with a view to provide a legal framework for cross-border recognition and interoperability of **secure eAuthentication systems**;

Key Action 16: Propose by 2012 **a Council and Parliament Decision** to ensure **mutual recognition of e-identification and e-authentication** across the EU based on online 'authentication services' to be offered in all Member States (which may use the most appropriate official citizen documents – issued by the public or the private sector);

Conclusions



STORK – eID interoperability

THANK YOU FOR YOUR ATTENTION

info@eid-stork.eu