BUILDING International Cooperation
for Trustworthy ICT

WG2 2.7: Implications arising from identity and privacy related issues on a global scale

Alberto Crespo, Atos Spain S.A.

International Drivers

Technical evolution: Internet of Things, Mobility, Cloud Computing…

Enhanced cross-border information flows: multinational companies with branches, ecosystem of complex relationships (customers, providers, partners…) where personal data of physical persons, legal person representatives, civil servants, etc. requires adequate protection.

Need for better identity and data protection on the Internet manageable *as a service*: fostering trust in eServices is essential.

Cybercrime and different security and privacy large-scale threats, esp. identity-related crimes, profiling, tracking, etc.

Demands from government, industry, NGO's, commerce institutions, standardisation bodies:

- **Effective engineering and technical solutions (e.g. PETs) to embed privacy by default and into the design of ICT systems.**
- **Interoperable electronic and Internet-based identity schemes allowing federation and cross-border, cross-domain, cross-sector interactions.**
- **Privacy respecting identity management involving private and government third parties: identity/attribute providers, service composition… Consistent metrics and assurance levels needed.**
- **Complexity of e-Relations requires not only dependable ICT infrastructure but articulating mechanisms for accountability, liability, audit, compliance monitoring, enforcement… across hetereogeneous legal and trust domains.**

People-Centric Drivers

- **Empowering the user for effective decision making on release of identity & personal attributes**
  - **Universal applicability of data protection/privacy principles and rights (OECD, 2009 'Madrid Declaration'…) i.e. proportionality, purpose specification, lawfulness/fairness… access, rectification, deletion, objection…**
  - **EU Data Protection Directive & new Data Protection Regulation for transfers to non EU countries**
  - **Effective feeling of being in control, having choice: digital sovereignty concept**
- **With exceptions: state legislation related to interests of 'national security, public safety or health, protection of other freedoms/rights…'**
- **Authentication strength (combine multiple AuthN factors). e-Signature comparable to standard signature when needed.**
- **ID data quality/accuracy: reliable sources (eID, IdP/AP…), LoA's**
- **Protect identity in some contexts: pseudonimity, anon. credentials (IdeMix, U-Prove), claims-based assertions (e.g. Is age over)**
- **Demand for adequate mgmt of unambiguous/informed consent and associated mechanisms (privacy notices, clear privacy policies and evidence of their enforcement, etc.): proportionality principle!**
  - **Data Type / Data Value consent**
  - **Destination (country, controller, application) and purpose of collection**

International Initiatives on eIDM

EU Draft Regulation on eID & Trust services

US NSTIC

Trusted credentials

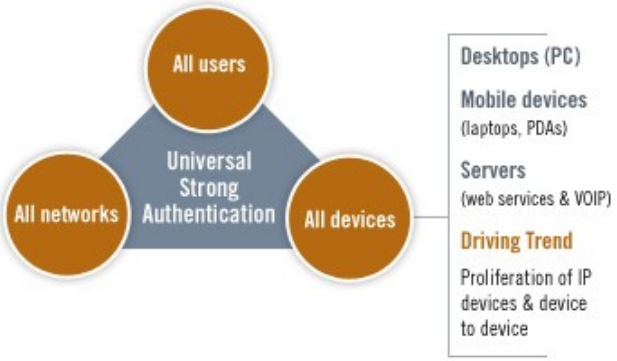
Private-sector led

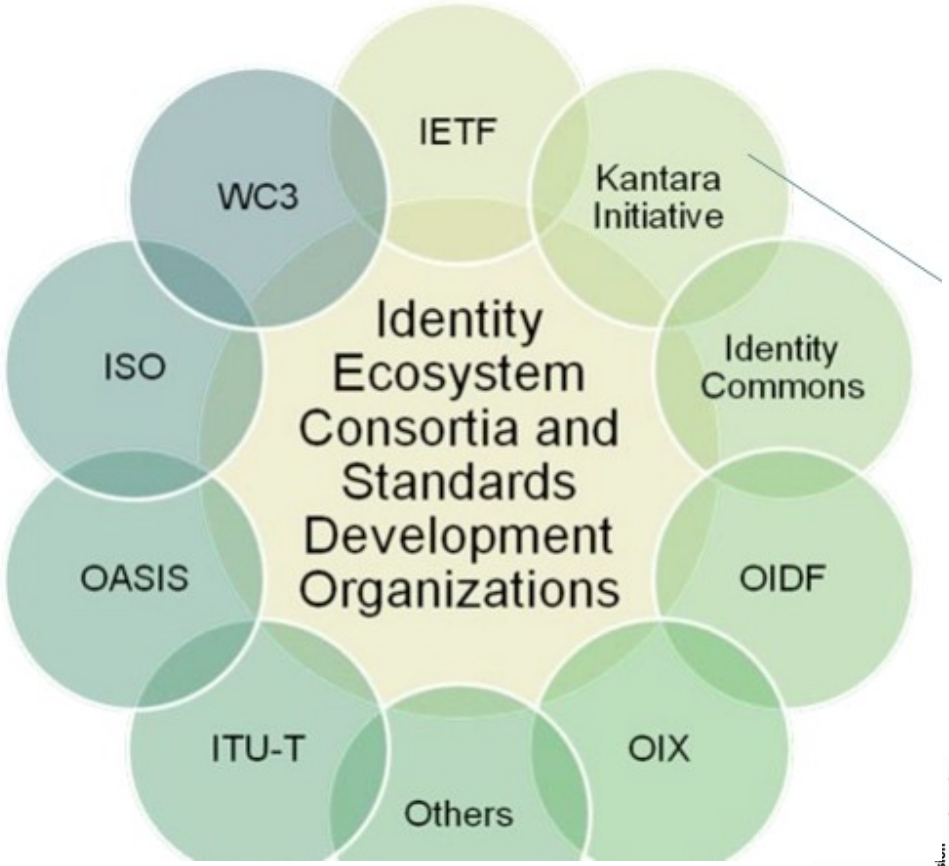
User-centric, voluntary

Kantara Initiative

OATH

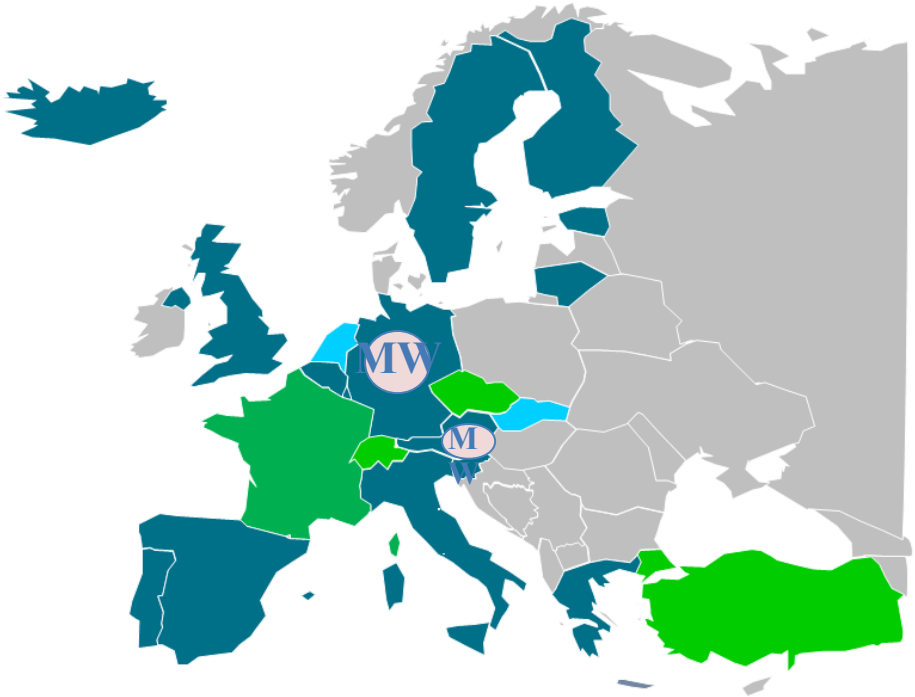
Strongly Authenticating Everyone, Everything, and Everywhere





[4]

EU ID Approach: STORK/STORK 2.0



STORK-1 MS IN PRODUCTION

STORK-1 MS IN PREPRODUCTION

OTHER STORK-1 MS

NEW STORK 2.0 MS

- 29+ Portals in 6 pilots
- 110+ eIDs accepted
- Succesful integrations: ECAS, PSCs, ECRN, SEMIRAMIS, eduGAIN…

eID for legal persons, Mandates, eID as a Service Offering, ext. attributes exchange

STORK2.0
SECURE IDENTITY ACROSS BORDERS LINKED 2.0

BUILDING International Cooperation for Trustworthy ICT

European Commission
Information Society and Media

Summary on Achievements of Objectives and Building a Long Term Strategy

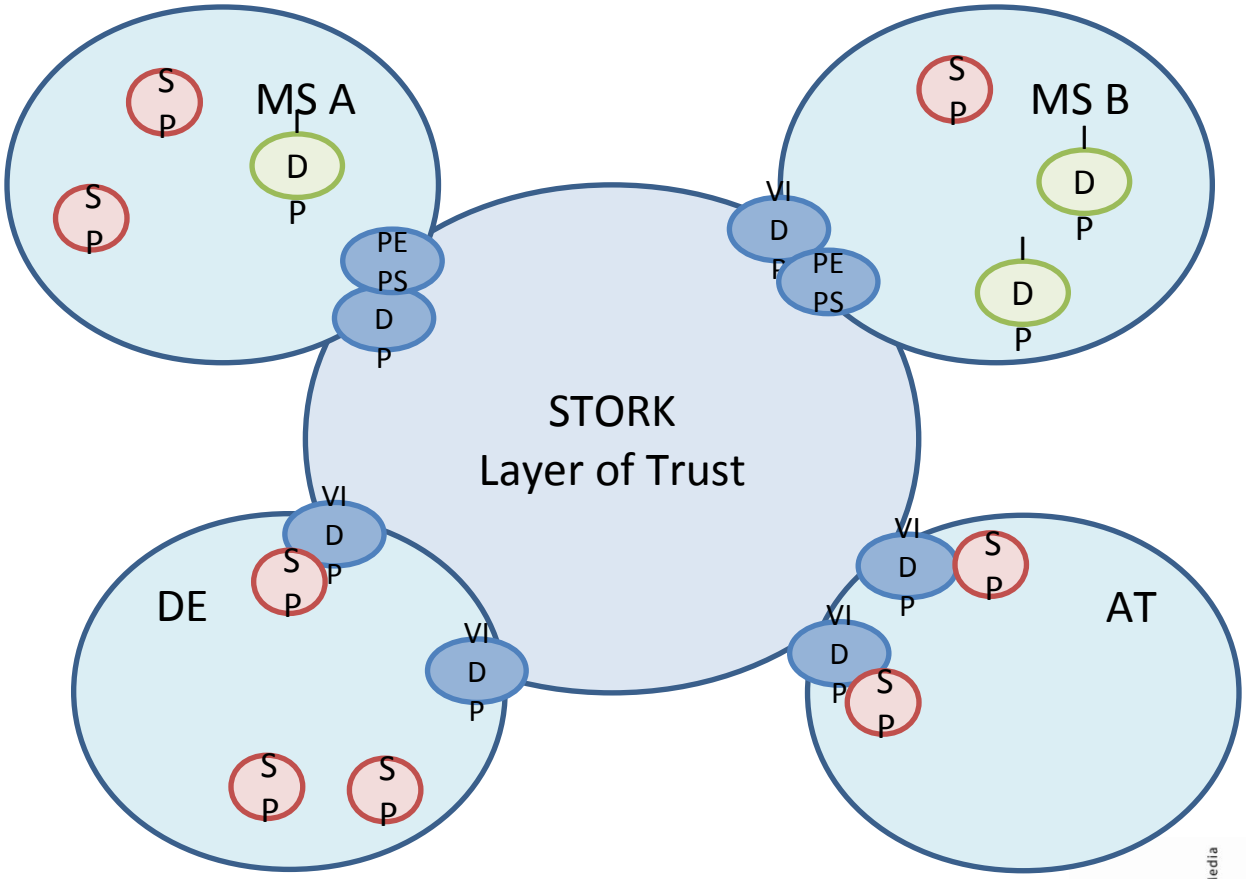
ABC

PEPS and V-IDP hide national specifics for other countries,

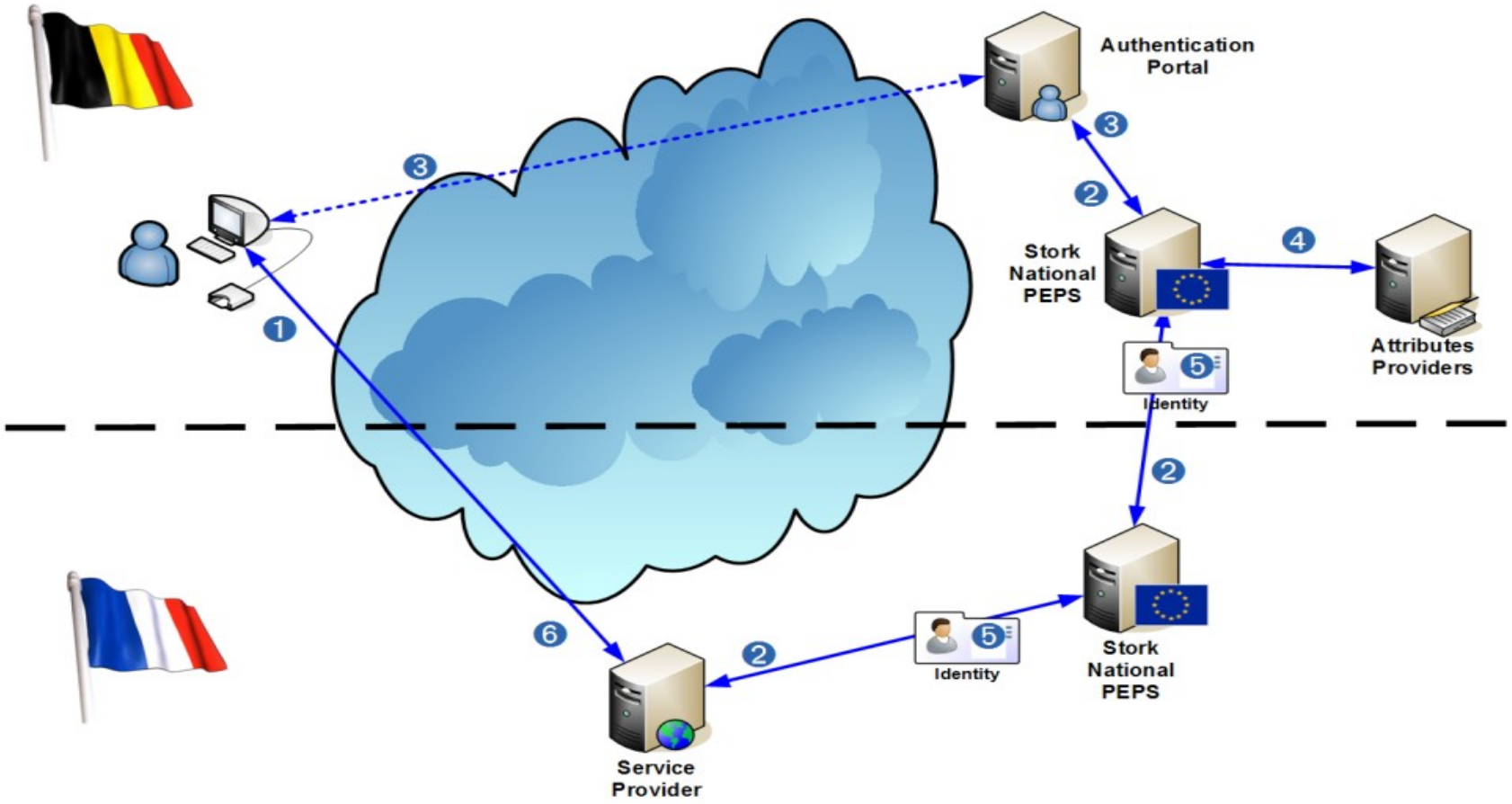
Co mm uni cati

C o m m

E l e



BUILDING International Cooperation for Trustworthy ICT



1. Citizen connects to Service Provider
2. Request connection to originating country authentication provider
3. Authentication (eID card, userid/password, OTP, ...)
4. Additional attributes gathering
5. Certified identity is sent to Service Provider
6. Service open to citizen

Bases for Int'l Cooperation in Data Protection

'Madrid resolution' (agreement by worldwide data protection / privacy commissioners)

Set of principles and rights for effective protection of privacy

Clarification of legitimacy of processing, sensitive data

Facilitation of int'l flows of personal data

Bilateral agreements. EU-US: Safe Harbor (voluntary self-cert. to be listed by Dept. Commerce), PNR/financial data…

If you offer services to EU citizens then consider new EU General Data Protection Regulation:

- Adequacy decisions
- Safeguards / standard data protection clauses (adopted by EC/DPA)
- Binding Corporate Rules
- Contractual Clauses

Other Int'l Privacy Instruments

1980 OECD Guidelines

Convention 108 of European Council (42 countries signed)

2004 APEC Privacy Framework (voluntary, not monolithic)

Over 60 national laws: Canada, Argentina, Mexico, Colombia, Uruguay, South Africa, Morocco, Tunisia, Dubai, Israel, Australia, South Korea, NZ…

Brazil, India, US, China, Japan: no transborder flow regulation

Basis: Human rights (EU) vs commerce-based (APEC).

2 basic approaches: geography vs organisation-based.

2 default positions: no flow unless legal basis present vs allow data flows with powers to limit in some circumstances

Transborder data flows: risks and benefits (e.g. UAE Blackberry case, SP's in China, Canadian provinces and 'Patriot Act'…).

Data Protection Management Elements to Consider

- Minimize points where personal data is stored, e.g. a processor needn't be a controller too; privacy-friendly logs
- Data security measures (E2E signing...): threat analysis, sec.obj./reqs
- Strict control of personal data sharing but allow user to export data in standardised formats (no lock-in)
- If you are data controller, process sensitive data… conduct a PIA.
- Personalisation of services: benefit or danger?
- Allow user to track what happens to their personal data
- Misuse/abuse notification and redress procedures
- No storage beyond purpose of processing
- Right to be forgotten, consent withdrawal: how to handle it outside EU
- Regulations need to balance flexibility (that doesn't suffocate innovation and business) with effective protection of fundamental rights
- Consider national laws of data subject's country (e.g. ID numbers, access to attributes restricted to specific SP's in UK, DE…) and SP country law (territorial principle)
- Common understanding needed on terminology, responsibilities…
  - Data subject/owner
  - Data controller or responsible person
  - Data processor or processing SP, etc.

Some recommendations

Good privacy as business differentiating factor: at same price people choose privacy-friendly vendors (make privacy stand-out)

Consumers need a ‘choice menu’: personalised services that require identification, other services that minimise collection of personal data. Privacy notices with clear language so user can compare with other providers. Avoid abusing consent.

Support data portability (e.g. profile portability) subject to consent.

Bureaucratic restrictions (e.g. approvals/regulatory filings) unefficient

Encourage organisationally-based transfer mechanisms (i.e. BCR, codes of practice, targeted audits, privacy seals…).

Enforcement should focus more on transfers that have greatest risk

Guidelines needed for int’l understanding of concepts, i.e. ‘adequate’

Transparency: jurisdiction application (avoid frictions btw laws).

See OECD study, *Regulation of Transborder Data Flows under Data Protection and Privacy Law*

Other elements for int'l cooperation

A set of common minimum standards of data security rules and policies can be agreed and certified by mutually recognised third parties (or MoUs signed).

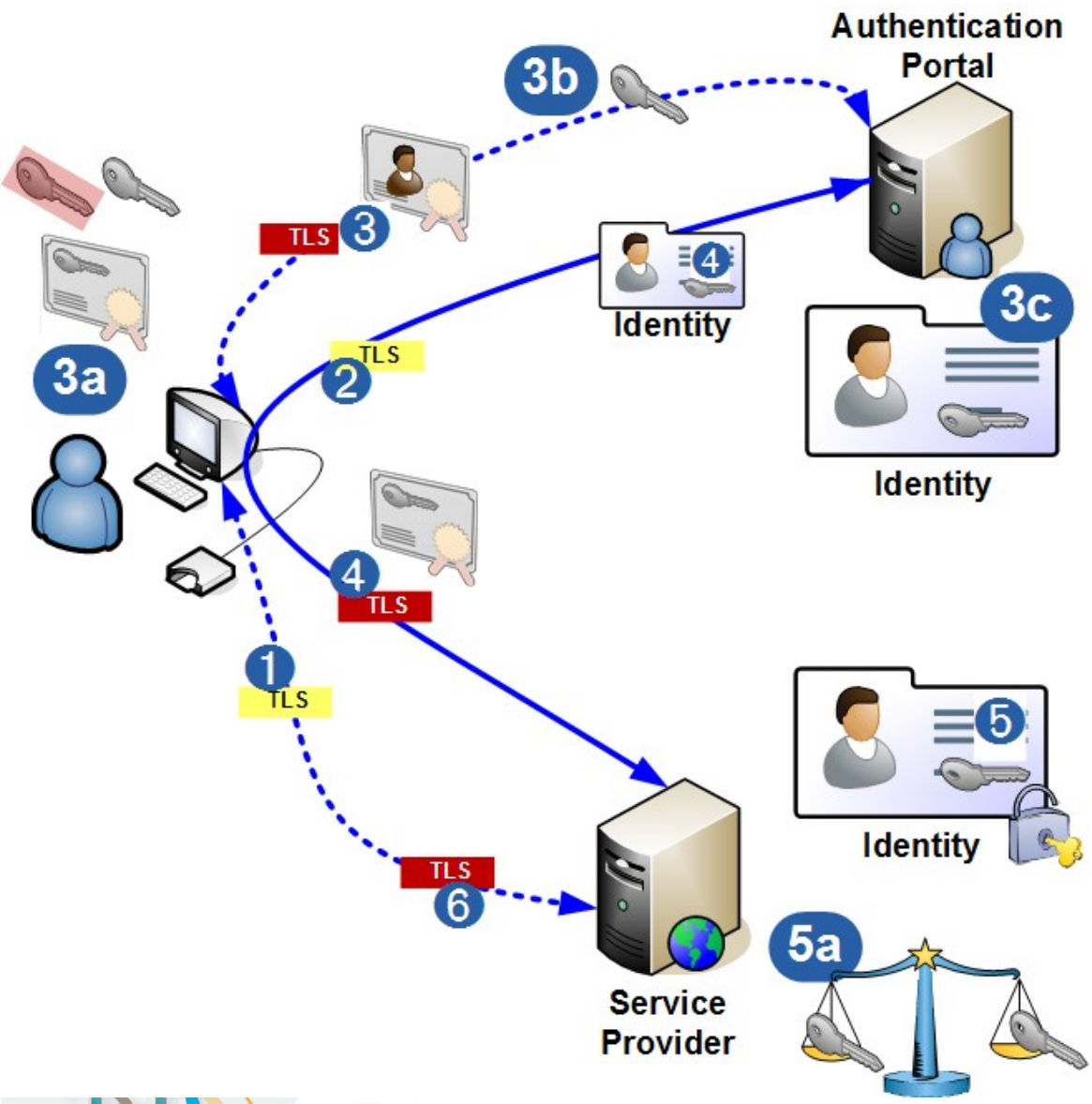
SLA's, liability for damages… complex to manage.

Data retention periods: different in different countries.

A common understanding on data minimisation / proportionality: need-to-know basis ambiguous, danger of attrib. aggregation.

End-user support: multilingual interfaces, accessibility compliance.

Technical IOP complexities: attribute names and values (semantics) can differ across contexts, representation of powers/mandates when acting on behalf of another person/company, trust in IDaaS contexts, giving consent to encrypted data sending.



1 Citizen connects to Service Provider

2 Request connection to originating country authentication provider

3 Authentication (eID card / X.509)

a) Key pair and certificate generation

b) Key sending inside secure connection

c) Key insertion in SAML signed assertion

4 Certified identity is sent to Service Provider

5 Assertion verification

+ compare keys from TLS connection and SAML assertion

6 Business transactions between citizen and service Provider with same key

Key binding could already begin during