DLA PIPER

EVERYTHING MATTERS

Authentication and Authorisation Infrastructures (AAIs)

Data Protection issues

Prof. dr Patrick Van Eecke

Universiteit Antwerpen - DLA Piper

Starting point: Identity Federation

"Provisioning user accounts for each application users wish to access does not not scale well in a highly distributed and collaborative environment that crosses multiple administrative domains and national boundaries"

"*More interactive, collaborative approaches to research in conjunction with the deluge of data are opening new frontiers to data processing, storing and preservation; this also poses new requirements and challenges for existing AAIs across Europe*"

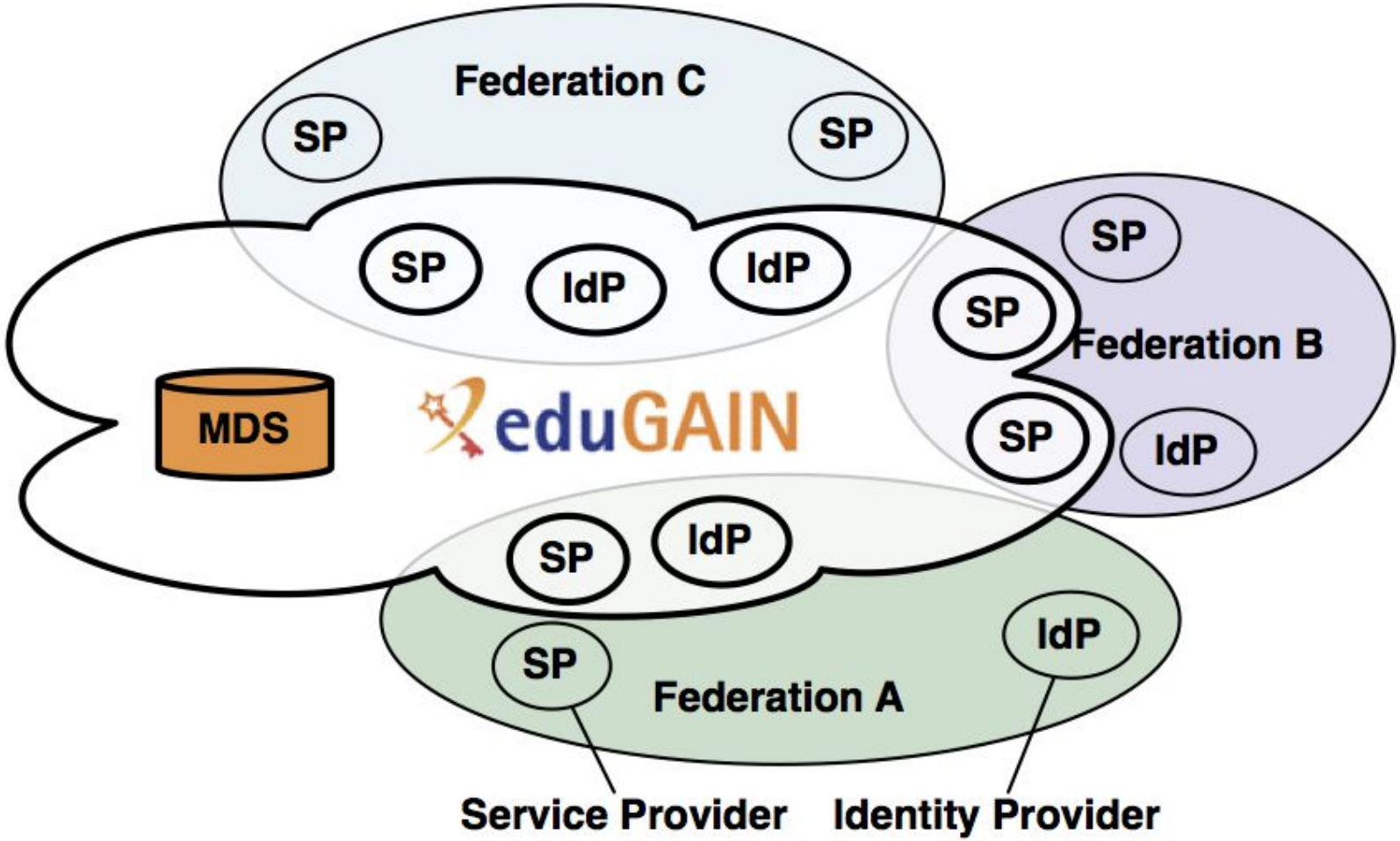
("Advancing technologies and Federating communities" Study on Authentication, Authorization and Accounting (AAA) Platforms For Scientific data / information Resources in Europe, 2012, p. 4 & 25)

Identity Federation

- An Identity Federation is an infrastructure where:
  1. **Authentication** is controlled by the user's **Identity Provider**, also referred to as IdP (typically the institution the user is affiliated with) that verifies the user's identity and issues access credentials (i.e. username and passwords, X.509 personal certificates etc.)
  2. **Authorisation** is controlled by the resource provider, also referred to as **Service Provider** (SP) or **Relying Party** (RP) that relies on the authentication done by the IdP and the information (attributes) received about that user from the IdP and possibly from other attribute providers within the Federation
  3. **Policy** or legal agreements are in place among the entities participating in the federation to achieve a trust relationship between the parties

(Advancing technologies and Federating communities" Study on Authentication, Authorization and Accounting (AAA) Platforms For Scientific data / information Resources in Europe, p. 25-26)

eduGAIN



eduGAIN technical architecture (courtesy of eduGAIN)

DLA PIPER

EVERYTHING MATTERS

The European legal framework

European legal framework

Treaty on the European Union

European Convention for the Protection of Human Rights and Fundamental Freedoms

Charter of Fundamental Rights of the EU

Data Protection Directive

Electronic Communications Privacy Directive

Data Retention Directive

Treaty on the European Union

*Article 16 (*ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

→ Common foreign and security policy

European Convention for the Protection of Human Rights and Fundamental Freedoms (1950)

- Article 8
  - Everyone has the right to respect for his private and family life, his home and his correspondence.
  - There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Charter of Fundamental Rights of the EU (2000)

Article 8 - Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Data Protection Directive

Official name

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Regulates:

- the manner in which personal data can be gathered in the EU;
- the rights of EU established citizens with respect to their personal data;
- the transfer of personal data to non-EU (EEA) countries.

Principles

- Notice
- Choice
- Onward Transfer
- Access
- Security
- Integrity
- Enforcement

Legal instruments (Article 249 EC Treaty)

- A Directive
  - shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.
- A Regulation
  - shall have general application. It shall be binding in its entirety and directly applicable in all Member States.
- A Decision
  - shall be binding in its entirety upon those to whom it is addressed.
- Recommendations and Opinions
  - shall have no binding force.

When does the directive apply?

- PROCESSING OF PERSONAL DATA
- *This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.*

- **Processing?**

- **Personal Data?**

When does the directive apply?

Processing

- collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment, combination as well as blocking, erasure or destruction of personal data

Personal data

- = any information relating to an identified or identifiable natural person
- an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- E.g. (name, adress, phone numer, ...)

When does the directive apply?

- Medium ?
  - Wholly or partly by automatic means

  OR

  - Manual filing of personal data form part of a filing system or are intended to form part of a filing system
    - 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

Key players

Data Subject

- an identified or identifiable natural person

Data Controller

- the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data

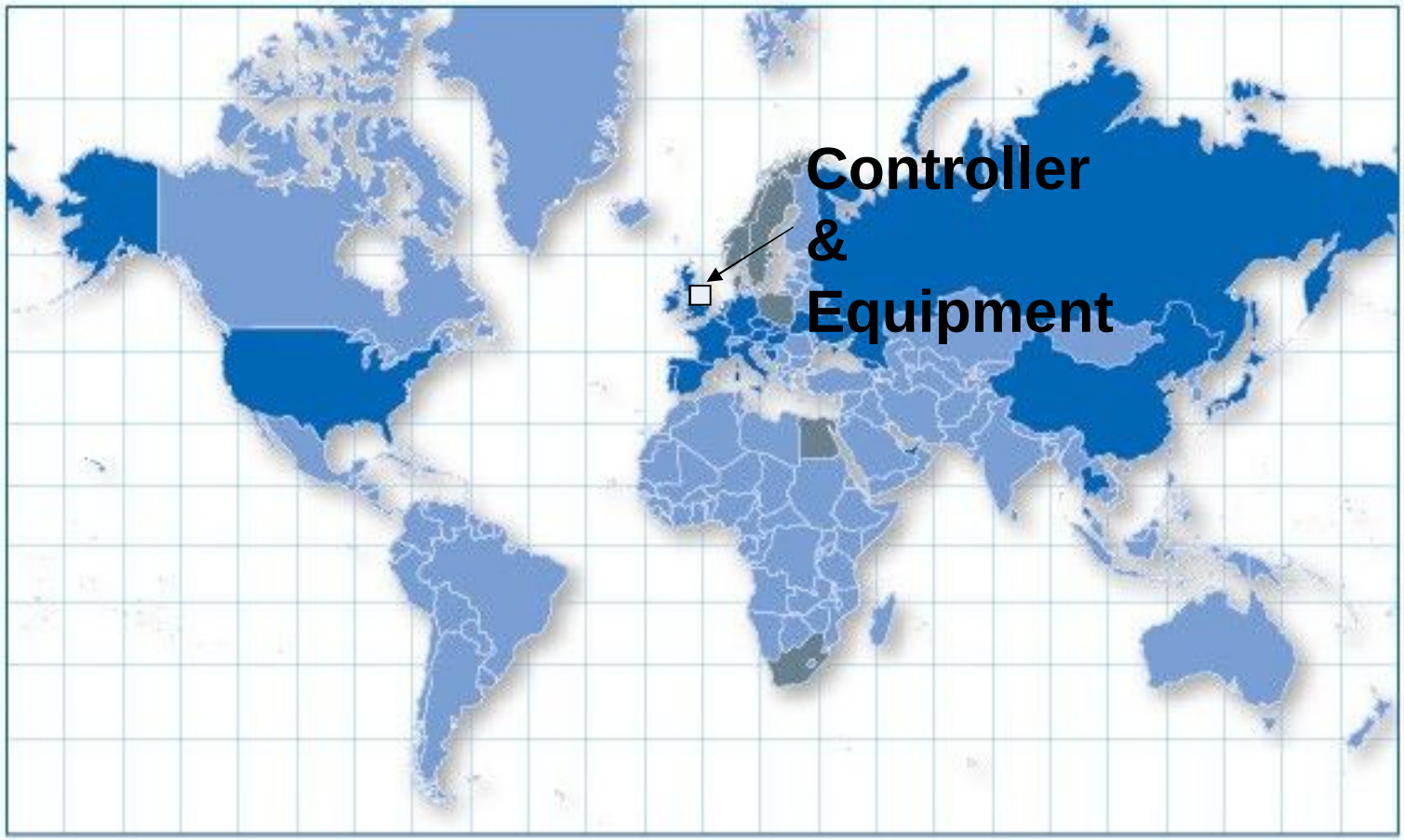
Data Processor

- a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

Where does it apply?

- The application of EU data protection law is not determined by the nationality of the data subject
- EU national data protection laws apply to:
  - Personal data controlled by entities established in an EU member state; AND
  - Personal data controlled outside the EU but processed using equipment in the EU.

Directive applies?



Directive applies?

Directive applies?

Directive does not apply?

Directive does not apply?

When can personal data be processed?

- ONLY IF …
  a) if the data subject has unambiguously given his consent;
  b) if processing is necessary for the performance of a contract;
  c) if processing is necessary for compliance with legal obligations;
  d) if processing is necessary in order to protect the vital interests of the data subject;
  e) if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;
  f) if processing is necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject

When can personal data be processed?

- "Sensitive data"
  - Medical
  - Religious
  - Gender
  - Political
  - …
- Special rules
  - Prohibited unless specific requirements fulfilled
    - E.g: Explicit consent
    - E.g: Processing only allowed by health care professional

Quality criteria for processing personal data

Personal data shall be:

1. Processed fairly and lawfully;
2. Collected for specified, explicit and legitimate purposes;
3. Adequate, relevant and not excessive in relation to the purposes (technical/organizational: state of the art);
4. Accurate and, if necessary, kept up to date;
5. Kept in a form that permits identification of data subjects for no longer than is necessary.

Information duties

- Towards goverment
  - notification to local Data Protection Authority

- Towards data subject
  - Data protection notice

    You should disclose to data subject in advance of processing:

    1. name of processor;
    2. type of data being collected;
    3. purpose for which collecting data;
    4. third parties to whom data may be released;
    5. intended uses of data by third party;
    6. data subjects right to object to additional processing;
    7. data subjects right of access and correction.

Security

All data should be held under circumstances that ensure:

- prevention of unauthorized access, disclosure, alteration, destruction of data;
- access of data only for a specific and valid purpose;
- by appropriate technical and organizational measures
  - Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
- E.g. ISO 17799.

Integrity of Data

- Data should be reviewed periodically to assure that it is still relevant.

- Data should not be retained longer than is necessary for purpose for which originally collected.

Automated individual decisions

- No decisions which produce legal effects concerning the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.
- Exceptions:
  - if that decision is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or
  - if that decision is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

Onward Transfer to third party

- Data subject has the right to:
  - know identity of any third party to whom data are disclosed;
  - object to certain processing;
  - receive information about uses by the third party and further transfer.

  - Regulated on Member State level

Access, correction and deletion rights

- Data subjects have right to :
  - access data held about them.
  - direct/indirect access
- Data controller has to
  - respond to the request within a reasonable period
  - for free/not for free
- Data subject can then:
  - request amendment of erroneous or inaccurate information
  - for free

Enforcement and Complaints

- Each Member State has a data protection authority (DPA)
  - Independent
  - Controlling authority
  - Sanctions
- Different rules and powers in Member States

EU Data Protection - Local variations

- Varying registration requirements
- Prior approval for ex-EEA transfers
- Security measures
- The type of information which is covered
- Consent
- Works council involvement
- Over implementation
- Enforcement and Criminal penalties
- Data Protection Officers

Harmonisation issues

- Issue: Divergent interpretation of law in that Member State;
  - enforce complaints about breach;
  - enforce the law.
- WP 29 tries to harmonize
  - National DPA's
  - EU DPA
  - Commission representative
  - Advisory status
  - Acting independently

Transfers to Third Countries

- Data cannot be transferred from the EEA to a third country unless ….

International data transfer

Main options for compliance

- Consent
- White list of countries
- EC Approved "model clauses"
- US Safe Harbor
- Binding corporate rules

Adequacy principle (art. 25)

- Adequacy: The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations;
  - particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

- The Commission may find that a third country ensures an adequate level of protection, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of negotiations, for the protection of the private lives and basic freedoms and rights of individuals.

Safe Harbor

- Safe Harbor
  - created because US does not have “adequate” privacy provisions;
  - requires certain procedures that must be adopted by US companies.

Alternative Basis

- EU Model Contract Clauses
- Corporate Binding Rules

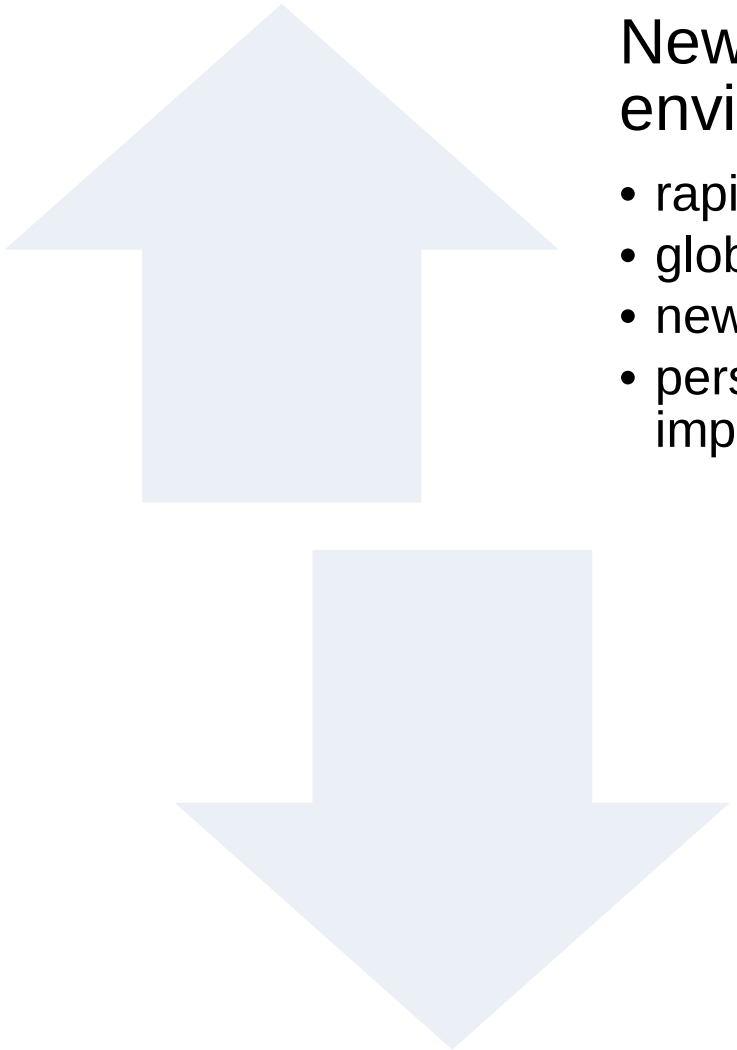
  - Recipient undertakes to provide substantially similar protection.

The story of Mrs Lindqvist

data protection hot issues

- **Data breach notifications**
- **The meaning of personal data**
- **On-line privacy:**
  - social networking/web 2.0
  - behavioural advertising
- **Cloud computing**
- **Data transfer and BCRs**
- **Data sharing and data access**
- **Balance between privacy and security**

Reason for change



New technical and social environment

- rapid pace of technological change
- globalisation
- new ways of information sharing
- personal data has become an important asset for many businesses

Current legal framework not able to cope with these challenges

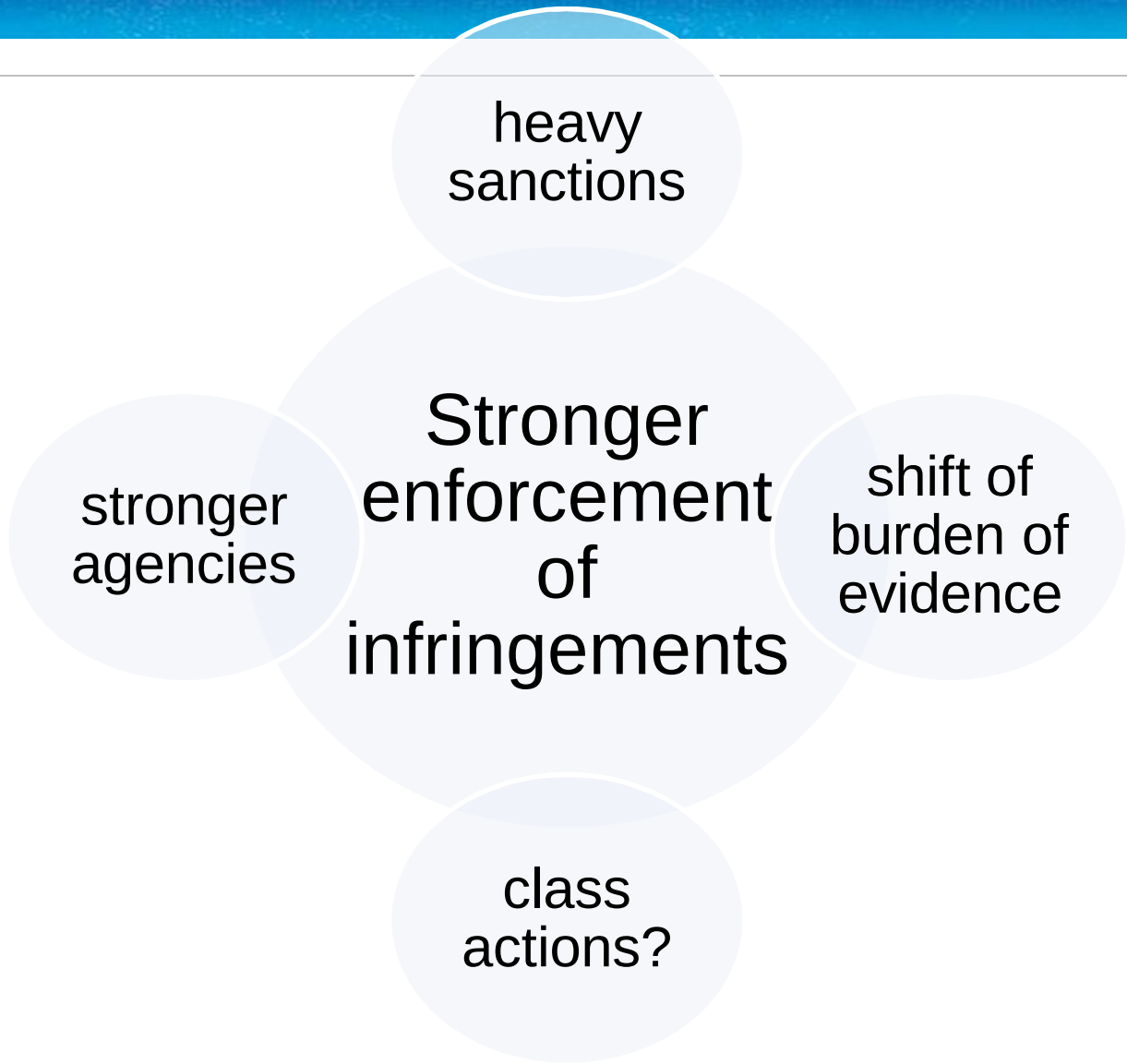
- does not provide the degree of harmonisation
- does not provide the necessary efficiency to ensure data protection

Review of the EU directive

- New rights
  - Right to be forgotten
  - Data portability right
- New obligations
  - Privacy by design
  - Privacy by default
  - Accountability principle
- Formal requirements
  - Less formal
- Enforceability
  - More harmonisation
- Third countries
  - smoother rules (BCRs)


right to be forgotten
privacy by default
data portability right
New rights for individuals
privacy by design
protection of children


data protection assessments
security breach notification
New obligations for companies
documentation requirements
data protection officer


heavy sanctions
stronger agencies
Stronger enforcement of infringements
shift of burden of evidence
class actions?

DLA PIPER

EVERYTHING MATTERS

Geant Code of Conduct

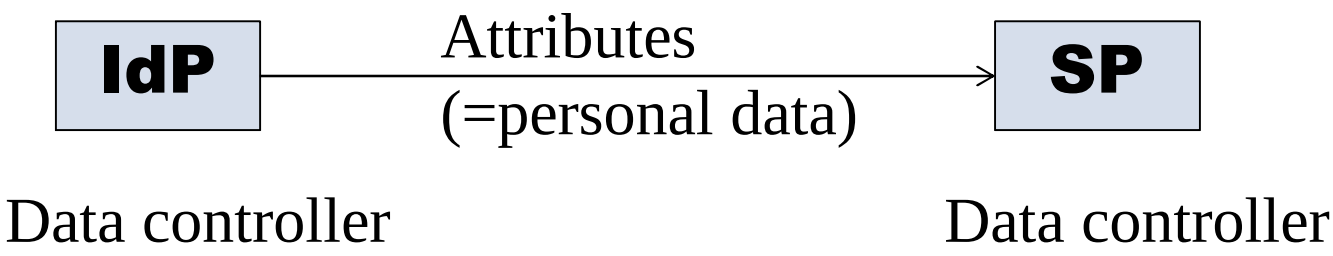
Context

- SPs want attributes
- Numerous European research SPs have expressed a particularly urgent need
- GÉANT exists to serve the requirements of European (not only national!) research & education

Background

- eduGAIN Data protection good practice profile 4/2011
  - Lawyer: not legally strong enough
  - => try to strengthen the framework
- Joined forces with the REFEDS attribute release workgroup
  - REFEDS is global, eduGAIN European initially
- Goal to develop a Privacy Code of Conduct
  - Make it generally approved by the community
  - Make it useful beyond Europe

The problem



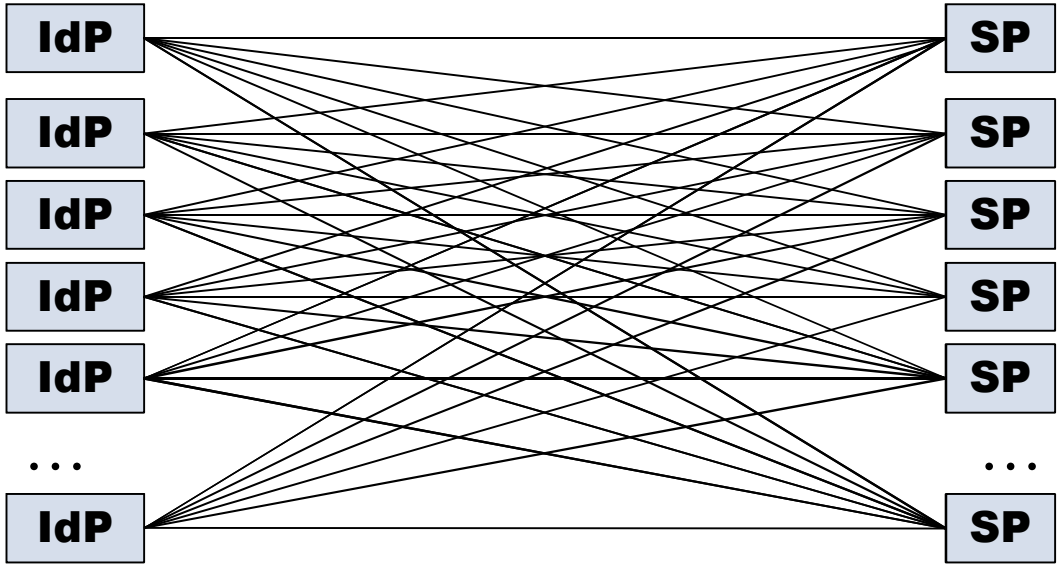
- IdP takes privacy risks when it releases personal data to an SP
- What if the SP gets hacked and personal data leaks to the Internet?
  - The regulator fines or end user sues the SP?
  - The regulator fines or end user sues the IdP??

=> To avoid risks, IdPs hesitate to release attributes to SPs

- Unless we manage to develop a framework which reduces the IdP risks

=> Privacy Code of Conduct

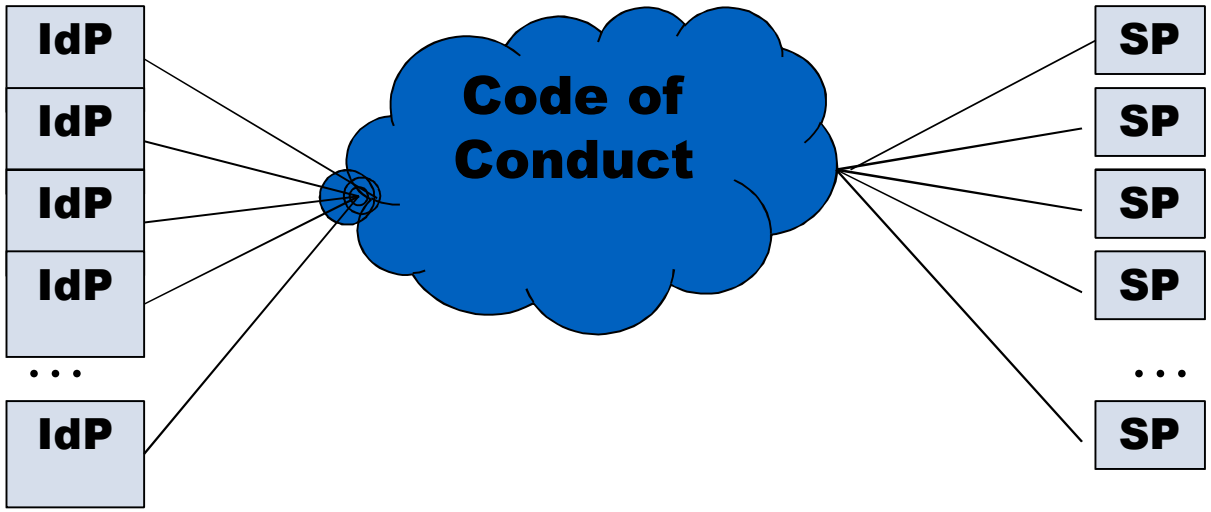
Abandoned solution: bilateral contracts between IdPs and SPs



- There are potentially hundreds or thousands of IdPs and SPs

=> bilaterals do not scale

The proposed approach



1. SPs commit to the Privacy Code of Conduct
   - Derived from the Data protection directive
   - Federation's SAML metadata is used to mediate the commitment
2. IdPs learn SPs have committed to the CoC
   - We hope that makes them less reluctant to release attributes

Requirements and limitations

Requirements

- **Balance the risks and the easiness of collaboration** for research and higher education
- Try to **avoid big changes** to current architecture (such as, existing federation agreements)
  - Would slow down adoption

Scope limitations

- Only **non-sensitive personal data** is released
- Limit to transfer **to EU/EEA countries** in the beginning
  - The General data protection regulation may ease release out of EU

The Data Protection Code of Conduct

- Introduction
  - To the data protection directive and its interpretation
  - To the approach adopted in the CoC
- Code of Conducts for SPs
  - + supporting guidelines: How to write a privacy policy. What attributes are relevant for a service.
- Good practice for IdPs
- Guidelines for federation operators
- Technical specifications
  - For SAML2 metadata
  - For an IdP-side attribute release module GUI

DLA PIPER

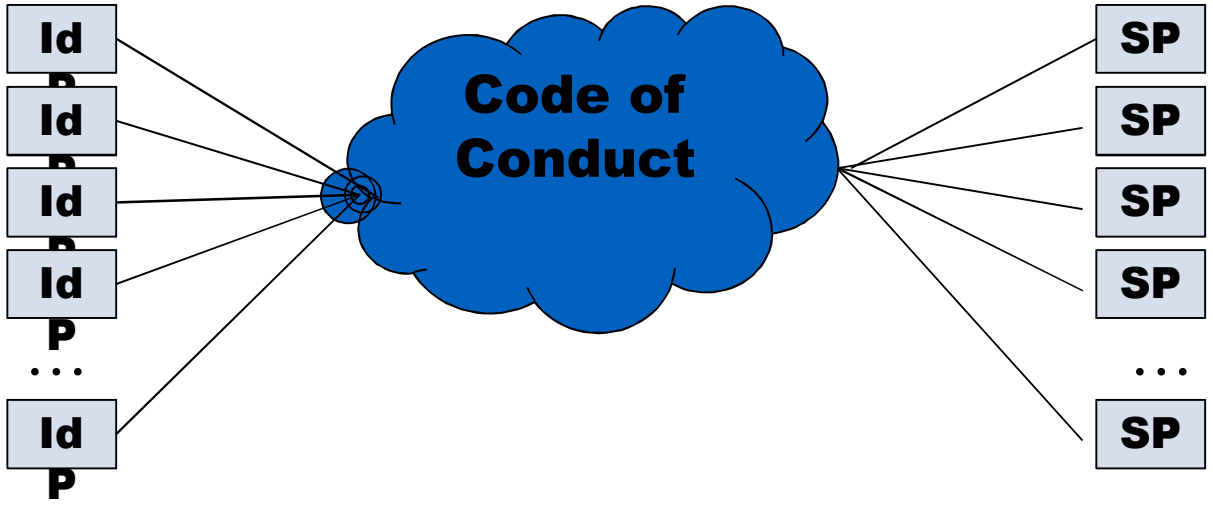
EVERYTHING MATTERS

Service provider requirements

SP Code of Conduct

- Data minimisation
  - Only strictly necessary attributes
  - Choose least intrusive option
- Grounds for processing
  - That necessary to deliver the service
  - Don’t offer the users extras
- Privacy statement available to the user
- Use of attributes
  - Only for access control and personalisation
- Security of information
  - Organisational and technical measures
  - Deleted when no longer needed

The big picture



Unilateral declaration or bilateral with central entity?

The options

Unilateral declaration

- Good
- Uses the model of the eduGAIN Declaration
- Quick and easy to implement and roll-out

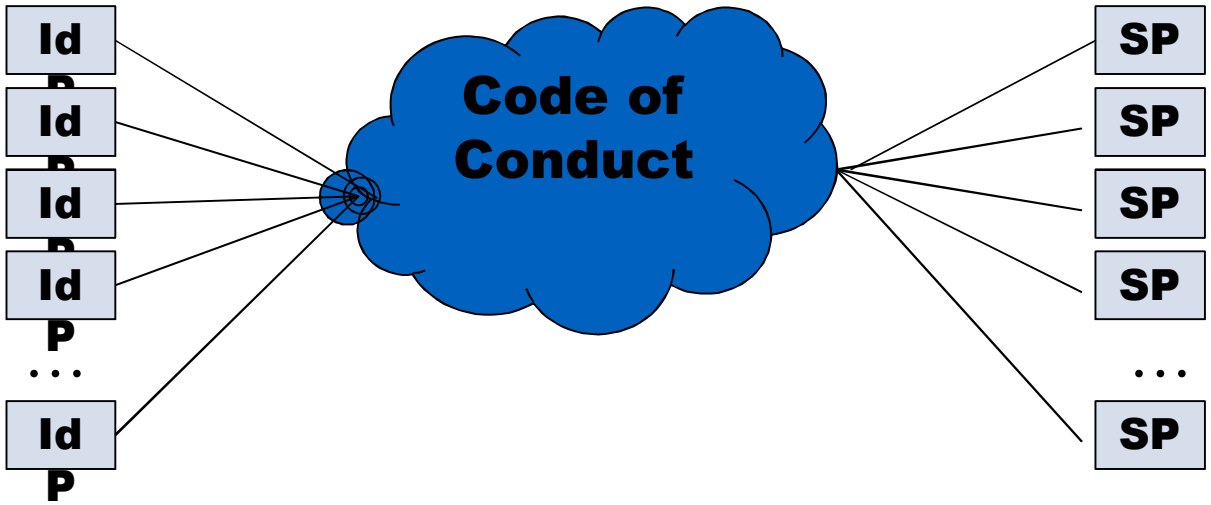
- Bad
- SPs may carry more liability than necessary

Bilateral

- Good
- Possibly more robust than a unilateral declaration
- Enables pairwise negotiation of responsibilities

- Bad
- Who is the counterparty?
- Relatively complex to roll-

The Big picture



1. The SP publishes its commitment to the Code of Conduct
2. The (inter)federation mediates the commitment to IdPs in the SAML metadata
3. An IdP learns the SP's and feels more comfortable to release attributes to the SP (we hope!)

Requirements for SPs

- Publish a signed (digitally/ink) CoC for SPs
  - Include a link to the document in the SAML metadata
- List the attributes required by the SP
  - Using RequestedAttribute elements in the SAML metadata
- Write and publish a Privacy Policy document
  - Link it from the SPs landing page
  - Reference it in the SP metadata (mdui:PrivacyStatementURL)
- Add other required SAML metadata elements
  - Mdui:DisplayName
  - Mdui:description
  - Mdui:logo
- Take care of your SPs security issues

Good practice for IdPs

- Decide if SP's commitment to the CoC convinces you to release attributes
  - Balancing your institution's risk appetit with the easiness of collabortion for your institutions researchers, teachers and students
- Decide how you want to onboard the SPs that have committed to the CoC
- Release only attributes that the SP Requests
- To reduce your data protection risks, you may decide to deploy an IdP-side attribute release module which shows to the user
  - The SP's name, description and logo
  - The SP's Privacy policy link
  - The list of attributes (name/description/value) to be released

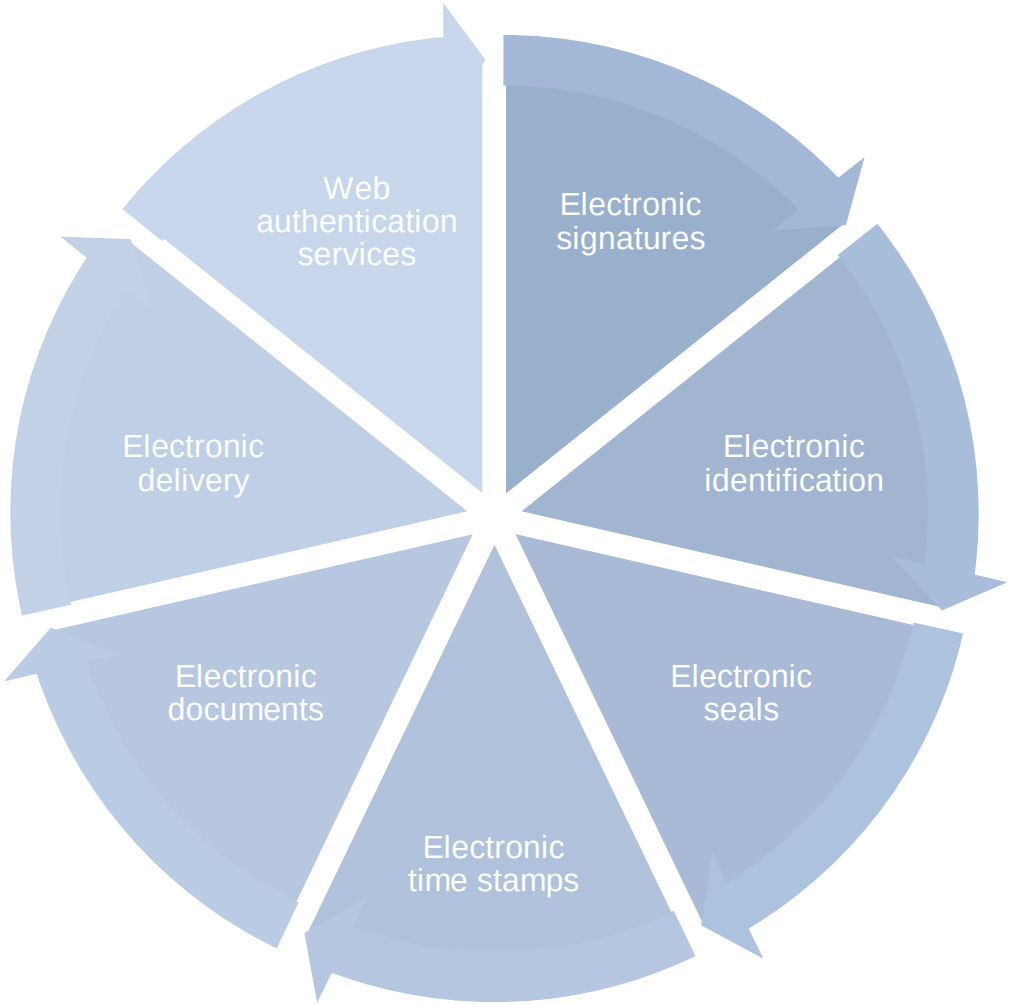
Operational issues for the federation

- In general, the federation(s) just mediate SP's SAML metadata to the IdPs
- In practice, it may be a good idea to support metadata management tools for IdP administrators
  - Tools that support the SP Code of Conduct
- Handling a misbehaving SP?
  - If an SP clearly not follows the CoC it has committed to

Next steps

Regulation of the European Parliament and of the Council on Trust and Confidence in electronic transactions in the internal market

Scope


Web authentication services
Electronic signatures
Electronic identification
Electronic seals
Electronic time stamps
Electronic documents
Electronic delivery

Principles

Notified eIDs

- Notified
- Mutual recognition
- eGovernment purposes

Qualified services

- Minimum of quality criteria
- Stronger supervision
- Publication of trusted lists

Legal effect

- Non-discrimination
- Equivalence (legal presumption)

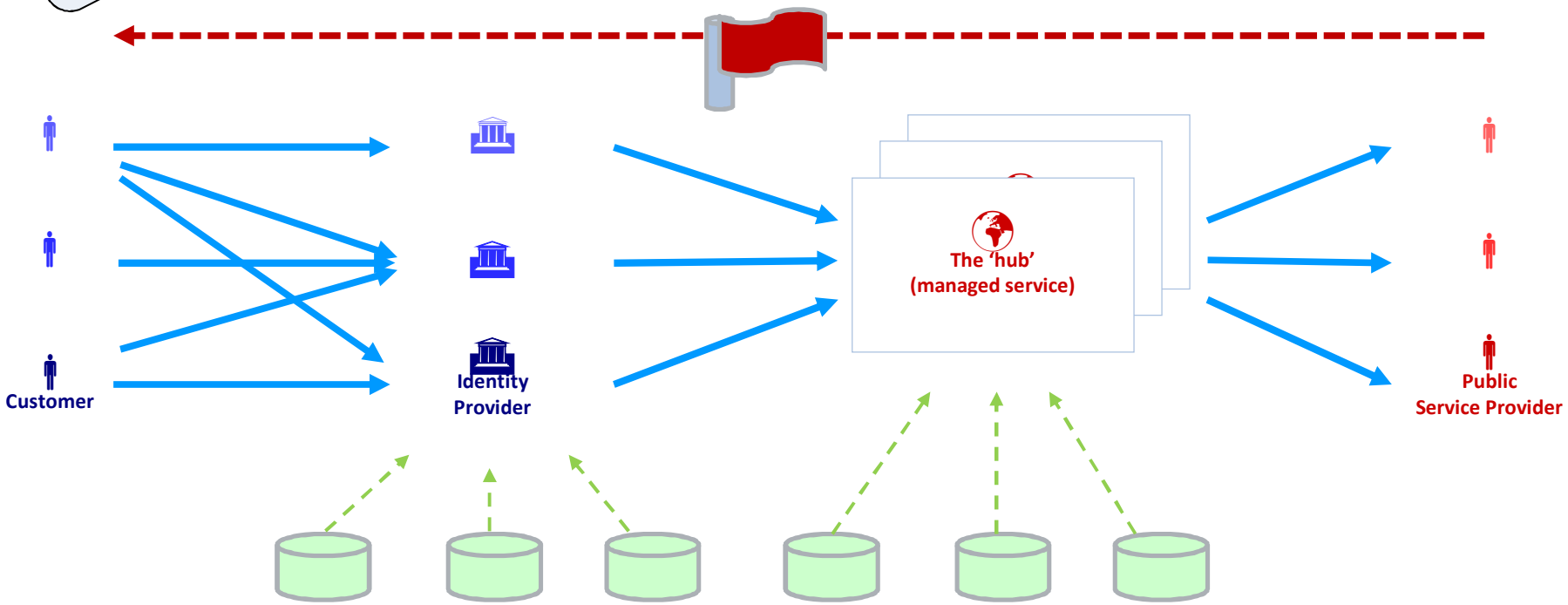
Standards

- Voluntary
- Conformity of compliance
- Published in OJ

- "electronic identification" means the process of using claimed set of data unambiguously representing a natural or legal person to deduce who the person is;

Cross Government approach to identity assurance

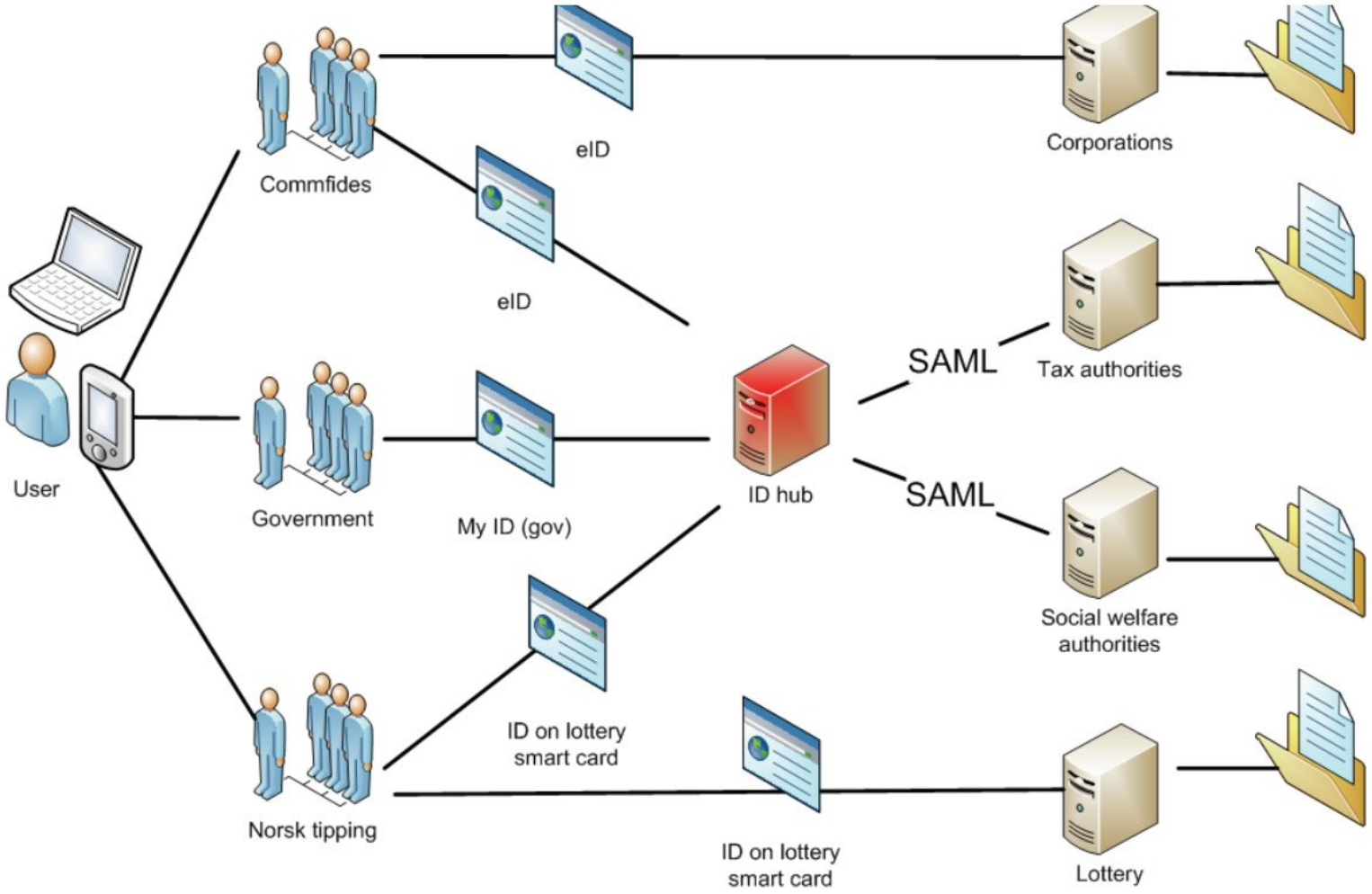
Ex. 1: eID project - UK



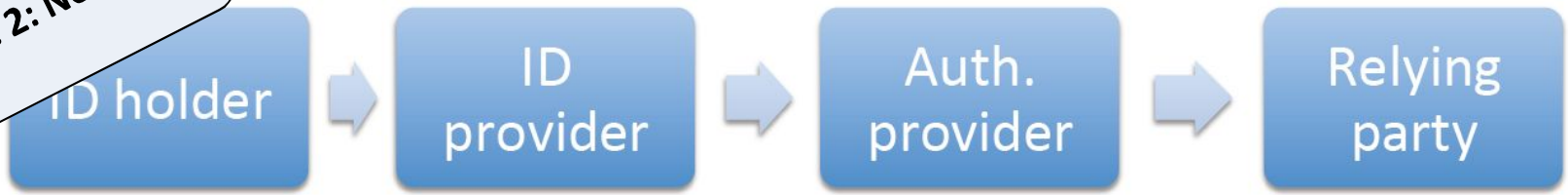
Identity assurance is only *one mechanism* for risk mitigation within the end-to-end transaction.

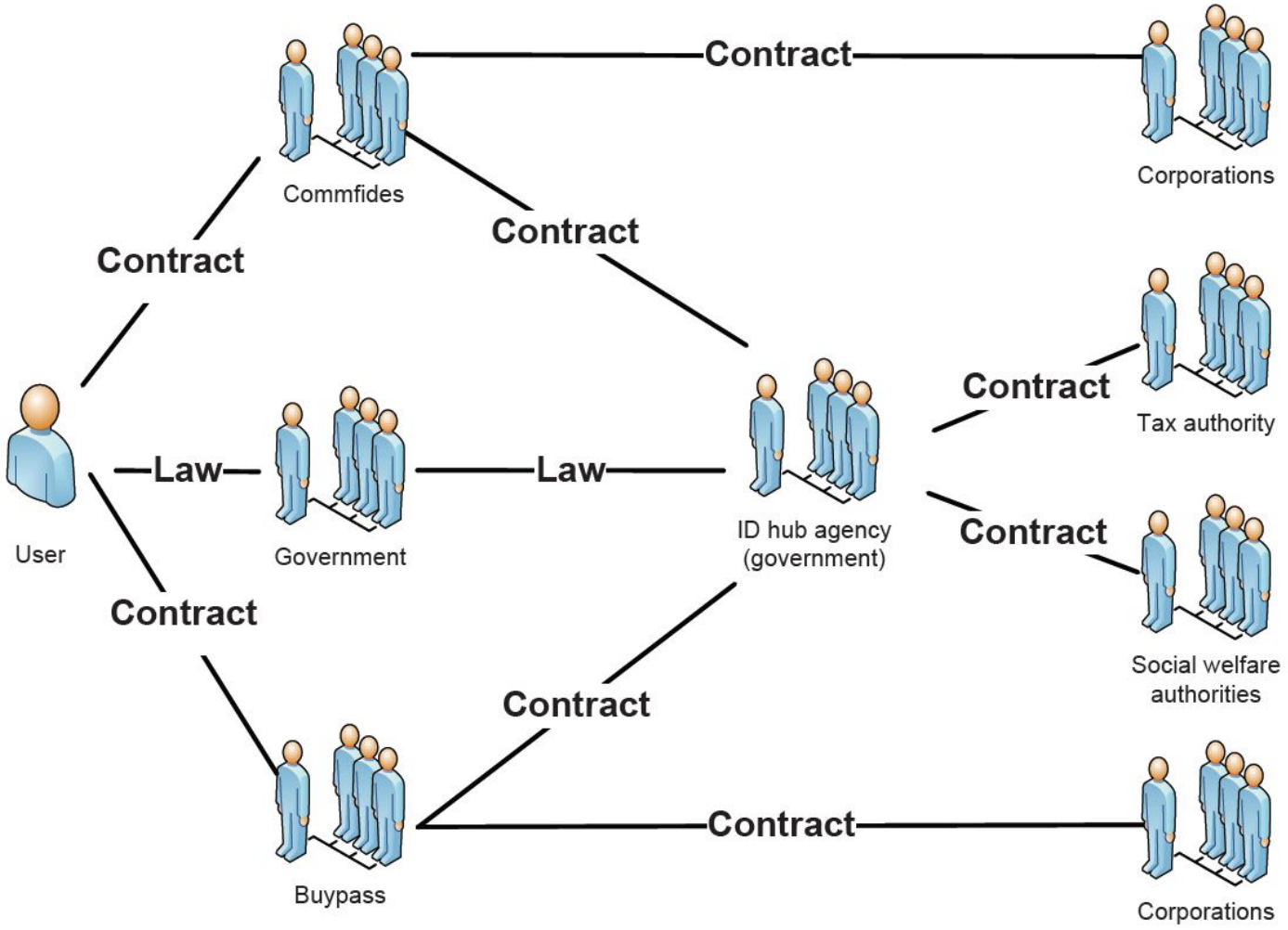
Slide re-used from Dr. Tobias Mahler, Norwegian Research Center for Computers and Law , with kind permission

Ex. 2: Norway



Ex. 2: Norway





Slide re-used from Dr. Tobias Mahler, Norwegian Research Center for Computers and Law , with kind permission

Ex. 2: Belgium, Austria, Portugal, ...

Centralised approach

Principles

Notified eIDs

- Notified
- Mutual recognition
- eGovernment purposes

Qualified services

- Minimum of quality criteria
- Stronger supervision
- Publication of trusted lists

Legal effect

- Non-discrimination
- Equivalence (legal presumption)

Standards

- Voluntary
- Conformity of compliance
- Published in OJ

eGov issue

- Member States may not request for public services an electronic signature with higher security insurance level than qualified electronic signature as laid down in this Regulation.

Example: qualified electronic delivery

- Data sent or received using an electronic delivery service shall be admissible as evidence in legal proceedings with regard to the certainty of the date and time at which the data was sent to or received by a specified addressee.
- Data sent or received using qualified electronic delivery service shall have the legal presumption of the date and time of sending or receiving the data.

Example: qualified electronic delivery

- Qualified electronic delivery service shall meet the following requirements:
- is provided by one or more qualified service provider;
- has unambiguous identification of the sender and if relevant, the addressee;
- the process of sending or receiving of data is secured by an advanced electronic signature or an advanced electronic seal in such a manner as to preclude the possibility of changing data undetectably;
- any change needed for the process of sending or receiving the data is clearly indicated to the addressee of the data.
- the date of sending, receipt and any change of data is indicated by qualified electronic time stamp or equivalent secure method;
- in case of the data is transferred between two or more qualified service providers, the requirements in (a)-(e) shall be applicable to all qualified service providers.

Conclusions

Next steps