Attribute-based Credentials for Trust

ABC4Trust impact on privacy – impact of the draft EU Regulation

Reference Group – 1st Meeting

Rüschlikon, 2012-02-13/14

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
Kiel, Germany

A research project funded by the European Commission's 7th Framework Programme

SEVENTH FRAMEWORK PROGRAMME

Overview

- ABCs for privacy (repetition)
- ABC4Trust in the current legal framework
- ABC4Trust and the European General Data Protection Regulation

What can we achieve with Privacy-ABCs?

- Data minimization:
  - issuance and showing are unlinkable
  - multi-show unlinkability
  - selective attribute disclosure
  - predicates over attributes

no additional linkability

selective can mean to the extent necessary

- Solution for typical scenarios that traditionally use (but not require!) identification / stating the name

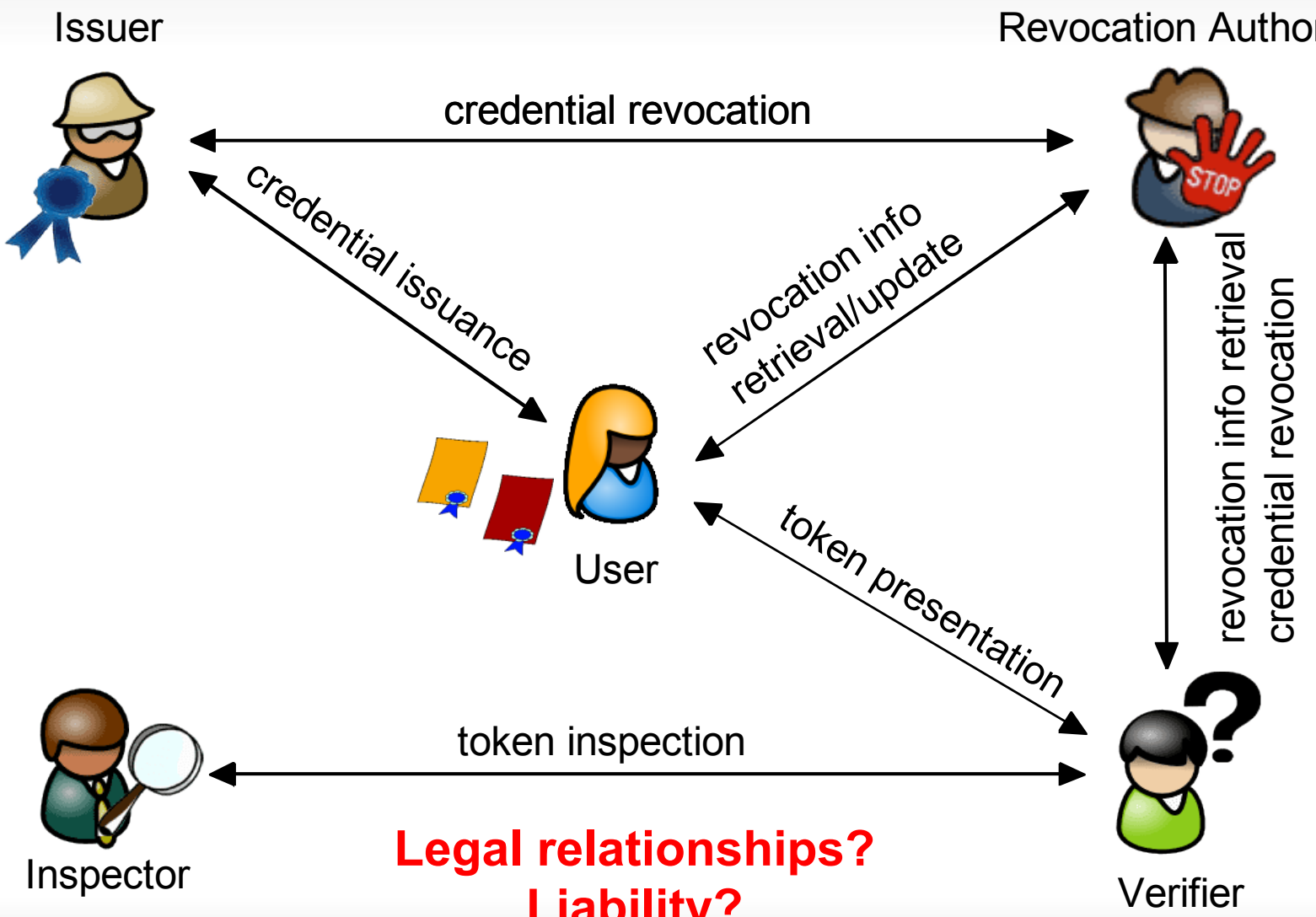
Compliance with data protection law?

- Possible;
  Privacy-ABCs are only one module in each use case
- No guarantee for privacy-friendly policies
- For compliance, Privacy-ABCs have to meet various requirements

Requirements for Privacy-ABC usage

- Fair & trustworthy interplay of all parties (esp. Issuer, Revocation Authority, Inspector) – not based on “blind trust”
- Transparency and intervenability for controllers, processors and data subjects
  - understandable information
  - sufficient control
- Only necessary attributes
- Sufficient size of anonymity sets
- …

Privacy-ABCs | Summary of Entities & Features



Slide from Anja Lehmann

Incentives in the current legal framework?

- Data minimization / separation of data not part of many DP Acts
  - Few exceptions, e.g. German Federal DP Act, but no sanctions

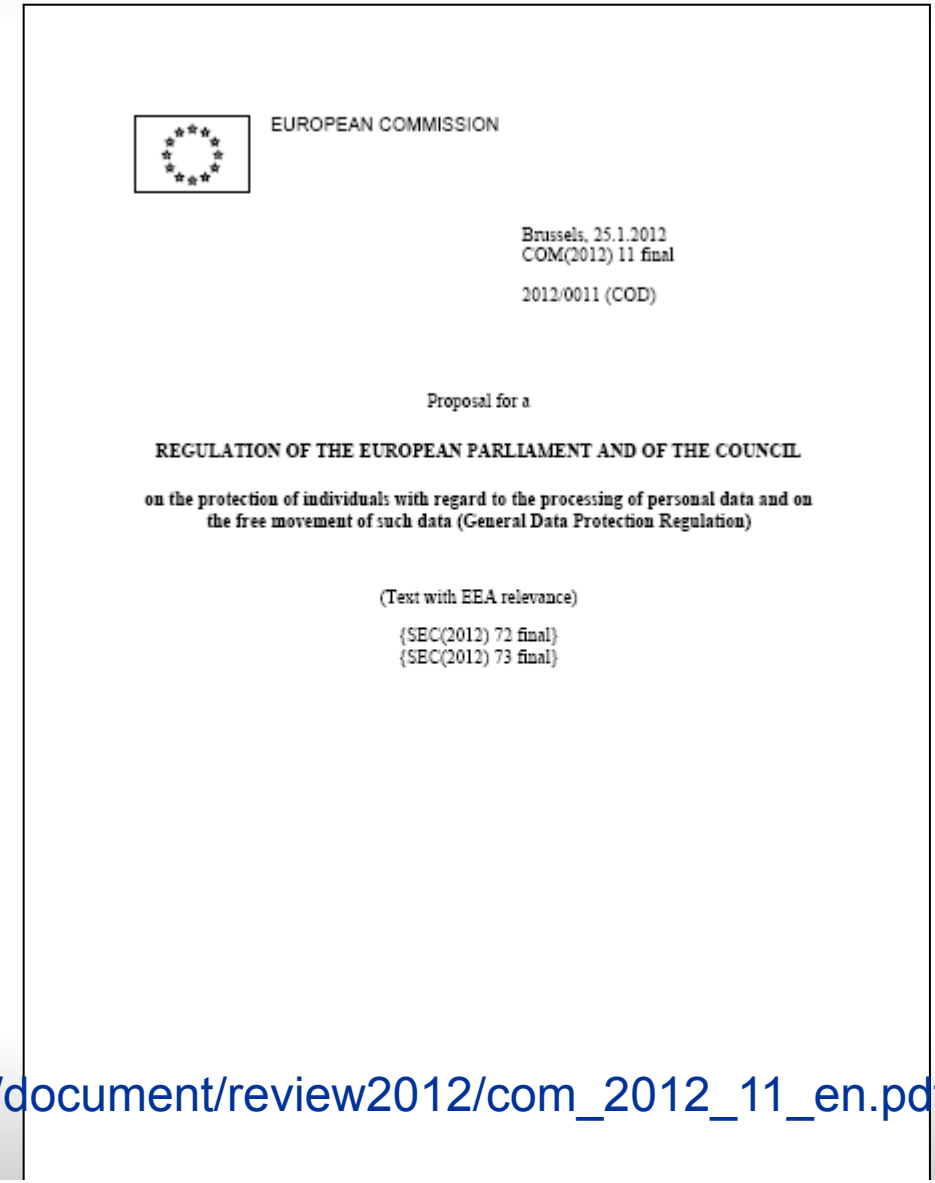
Revisions in (national) law required

- Data processing lawful if regulated by statutory provision OR consent
- 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.”

State-of-the-art: Hen-and-egg effect

European General Data Protection Regulation

- One regulation for all EU Member States
- Applicable without national implementation
- Draft issued January 25, 2012
- 91 Articles
- Currently: discussion phase



EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(Text with EEA relevance)

{SEC(2012) 72 final}
{SEC(2012) 73 final}

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Some highlights

- Art. 17: Right to be forgotten and to erasure
- Art. 18: Right to data portability
- Art. 20: Measures based on profiling

- Art. 3: Territorial scope
- Art. 22: Responsibility of the controller
- Art. 23: Data protection by design and by default
- Art. 10: Processing not allowing identification

First some definitions

Article 4 – Definitions

For the purposes of this Regulation:

(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

(2) 'personal data' means any information relating to a data subject;

[…]

Territorial scope

Article 3 – Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

   (a) the offering of goods or services to such data subjects in the Union; or

   (b) the monitoring of their behaviour.

[…]

Responsibility of the controller

Article 22 – Responsibility of the controller

1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.

[…]

Article 23 – Data protection by design and by default

1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

[…]

Data protection by design and by default

Article 23 – Data protection by design and by default

[…]

2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

[…]

Possibly: delegated acts

Article 23 – Data protection by design and by default

[…]

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.

[…]

Security of processing

Article 30 – Security of processing

1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.
2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.

[…]

Penalties / sanctions

Article 79 – Administrative penalties

[…]

6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2% of its annual worldwide turnover, to anyone who, intentionally or negligently:

[…]

(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;

[…]

Processing not allowing identification

Article 10 – Processing not allowing identification

If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.

A bit unclear:

“verification of the identity“

for the data subject ‘s right of access (Art. 15)

Summary

- Privacy-ABCs are only real Privacy-ABCs if the meet several requirements
- The European General Data Protection Regulation may be a means to promote privacy technology (better than before)
- But: Privacy-ABCs have to be understood + state-of-the-art + not too costly
- Caveat:
  possible legal obligations to store & link data + legal provisions that enable governmental access

Question to the experts (=YOU!)

What does this mean for ABC4Trust?

Thank you for your attention

Marit Hansen
Unabhängiges Landeszentrum für Datenschutz
Holstenstraße 98, 24103 Kiel
marit.hansen@datenschutzzentrum.de

ABC4TRUST

A research project funded by the European Commission's 7th Framework Programme.

SEVENTH FRAMEWORK PROGRAMME