Attribute-based Credentials for eIDs

Harald Zwingelberg
(Unabhängiges Landeszentrum für Datenschutz)

Commenting the proposal for a Regulation on Electronic Identification and Trust Services (eIDAS) under Privacy and ABC4Trust aspects

ABC4TRUST
A research project funded by the European Commission's 7th Framework Programme.
SEVENTH FRAMEWORK PROGRAMME

Overview

Attribute Selection - a necessary feature

Amendments introducing privacy aspects

I. Emphasize concept of authentication instead of identification

II. Remove barriers for privacy-preserving eID solutions

III. Data protection for eID chapter

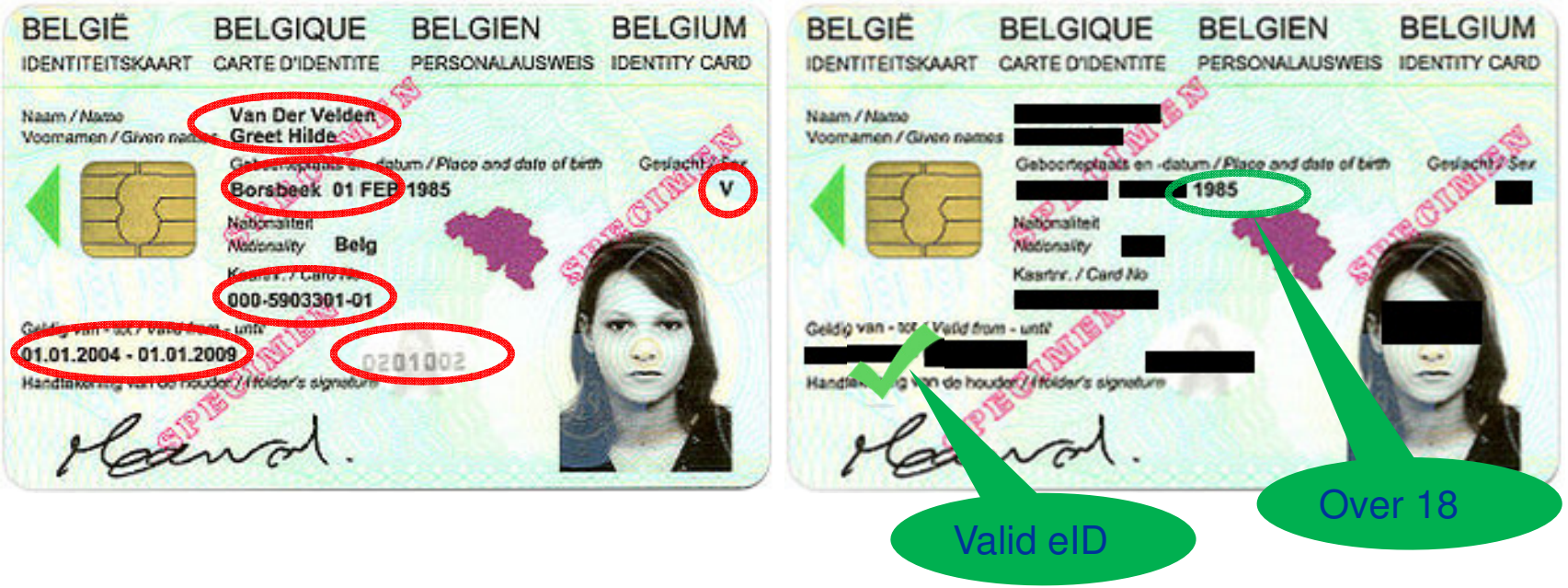
Attribute Selection

- Order alcohol online? Data to provide:

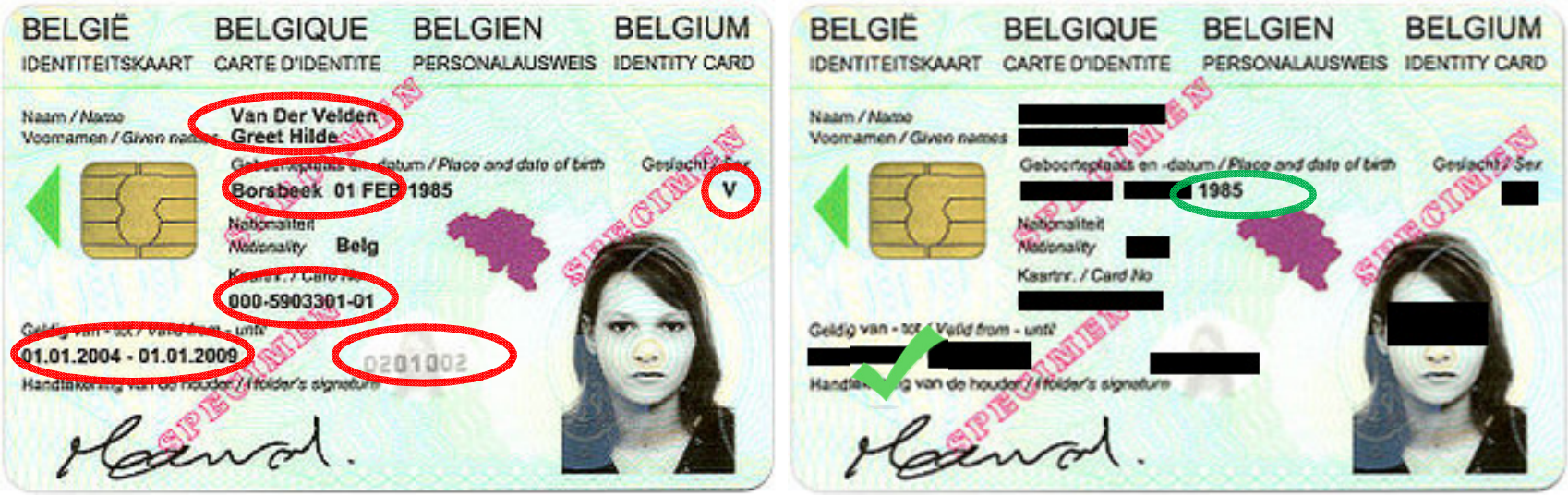
Status of many current eID solutions

Attribute Selection

- Order alcohol online? Necessary data:



Attribute Selection



Yes, we can!

And for the citizen's privacy we **must**!

Necessary privacy adjustments to the draft eIDAS regulation

I. Emphasize concept of authentication instead of identification

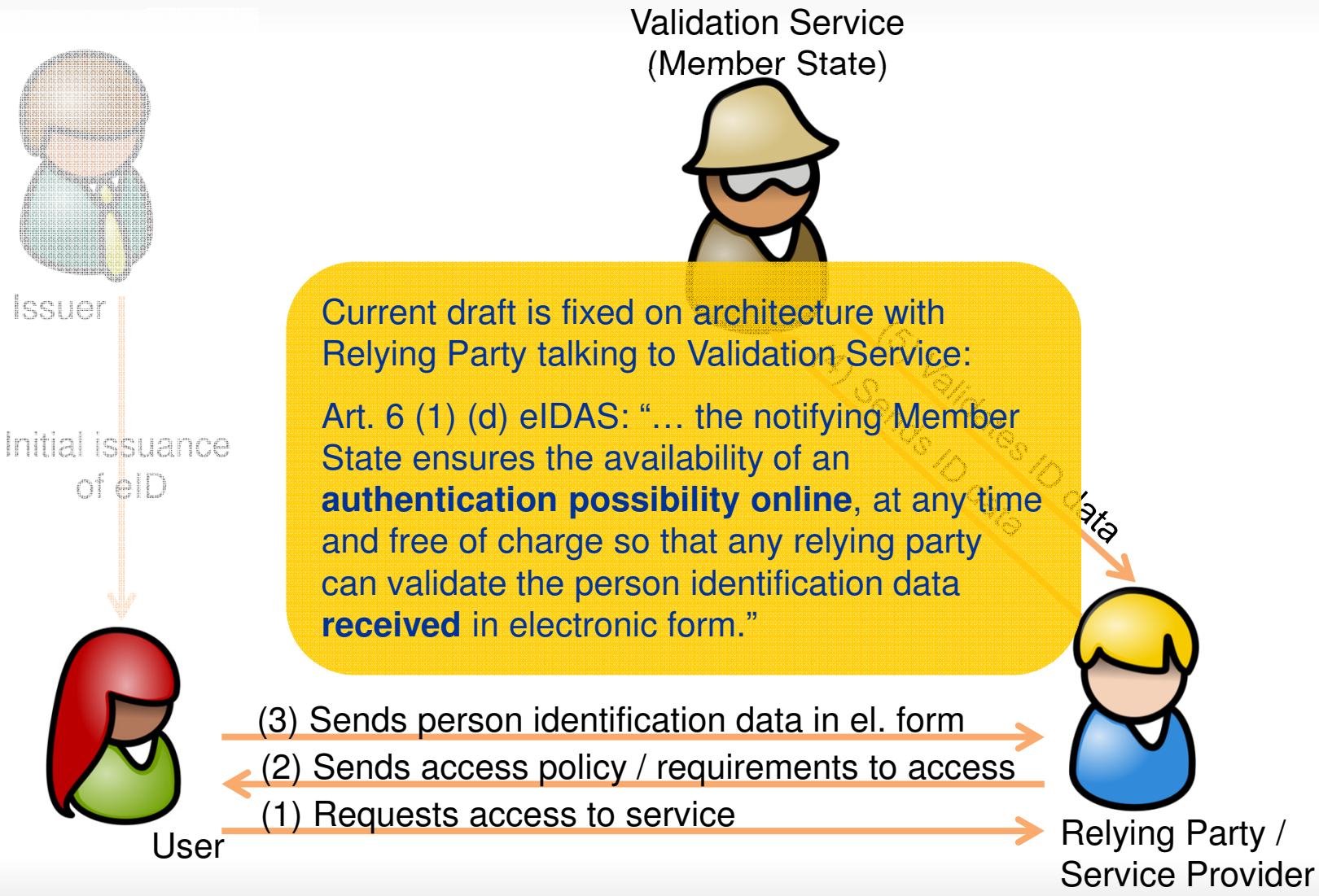
- Unlinkable authentication as basic use case only verifying necessary attributes (age, place of living, being a pensioner,…)
- Context specific authentication if it is necessary to verify that the same persons acts
- Identification with identifying attributes where knowledge of the identity is necessary

Necessary privacy adjustments to the draft eIDAS regulation

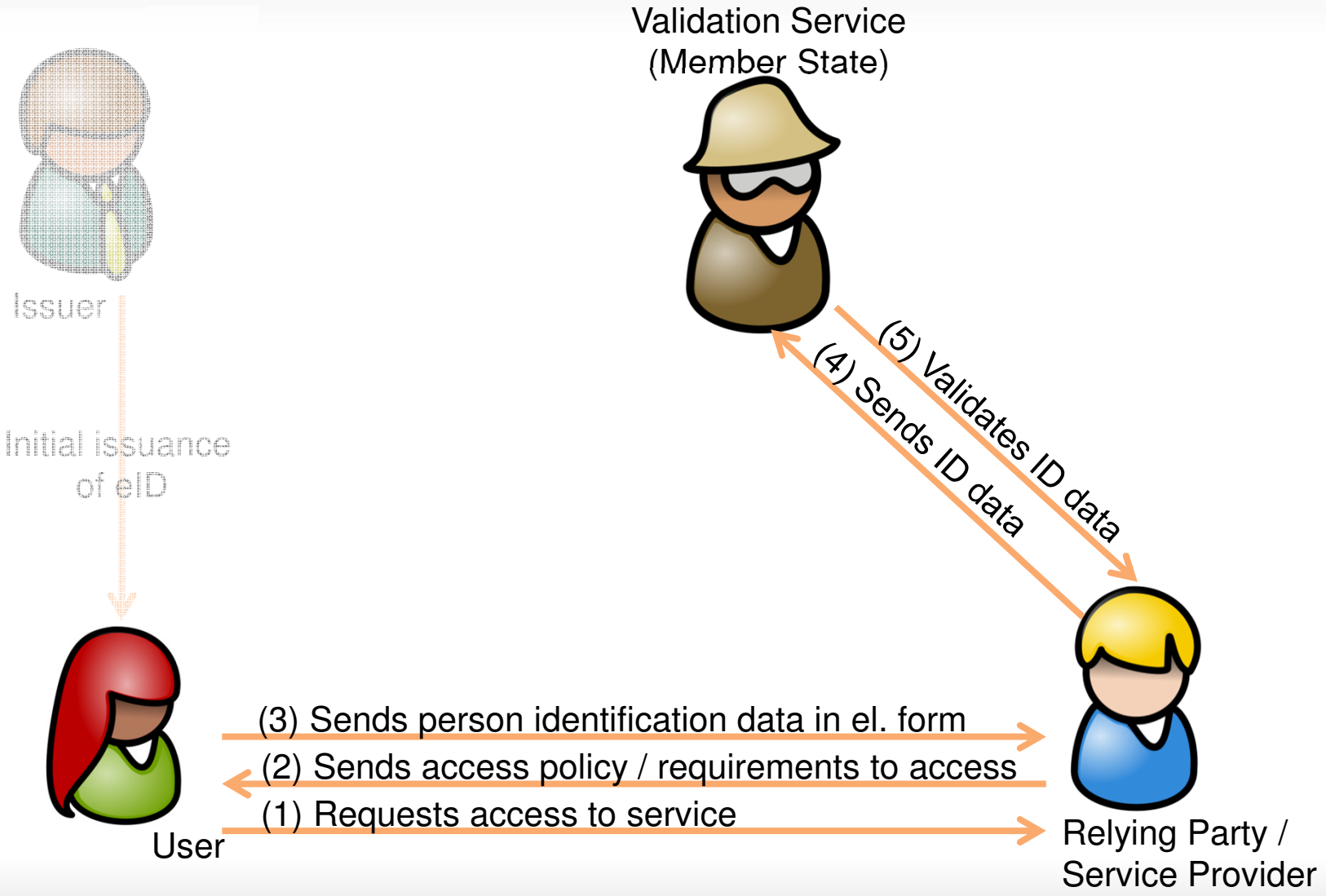
II. Remove barriers for privacy-preserving solutions

- Open eIDAS for privacy-preserving solutions
- No fixation on a single architecture
- Relying parties may be demanded to fulfill proportionate requirements
- Notifying Member States should ensure that validation is possible free of charge

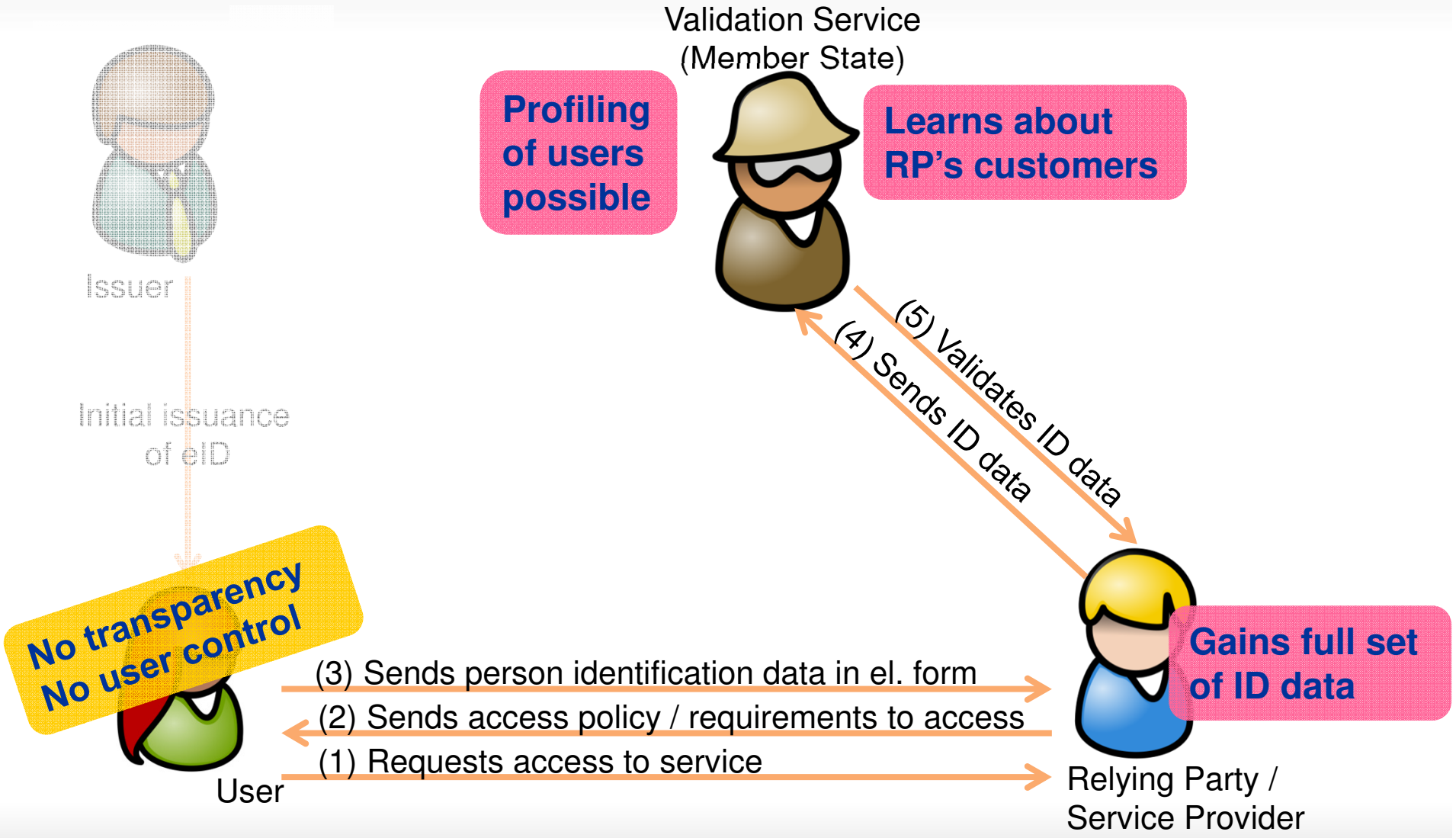
Current draft Art. 6 (1) (d) eIDAS



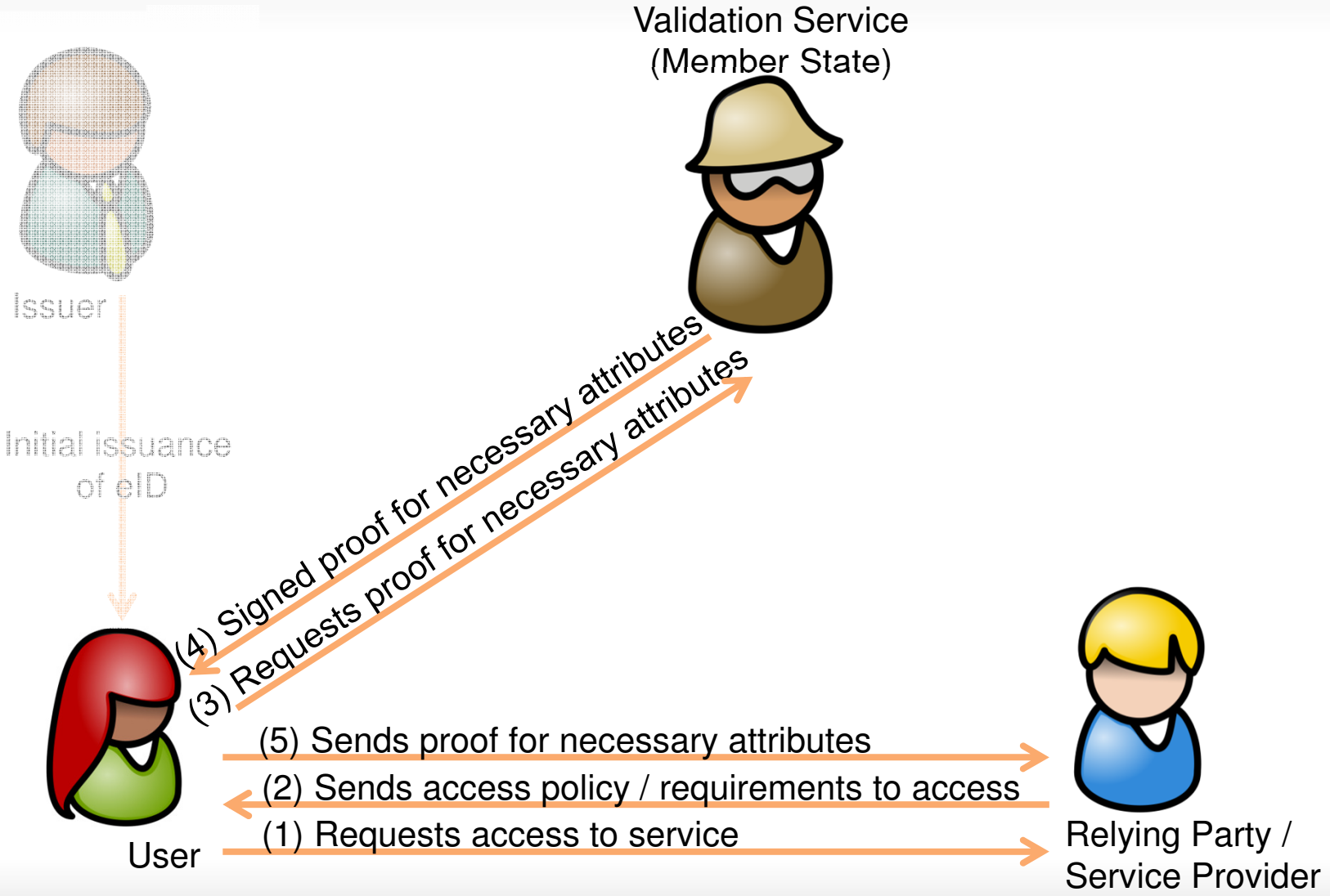
Current draft Art. 6 (1) (d) eIDAS



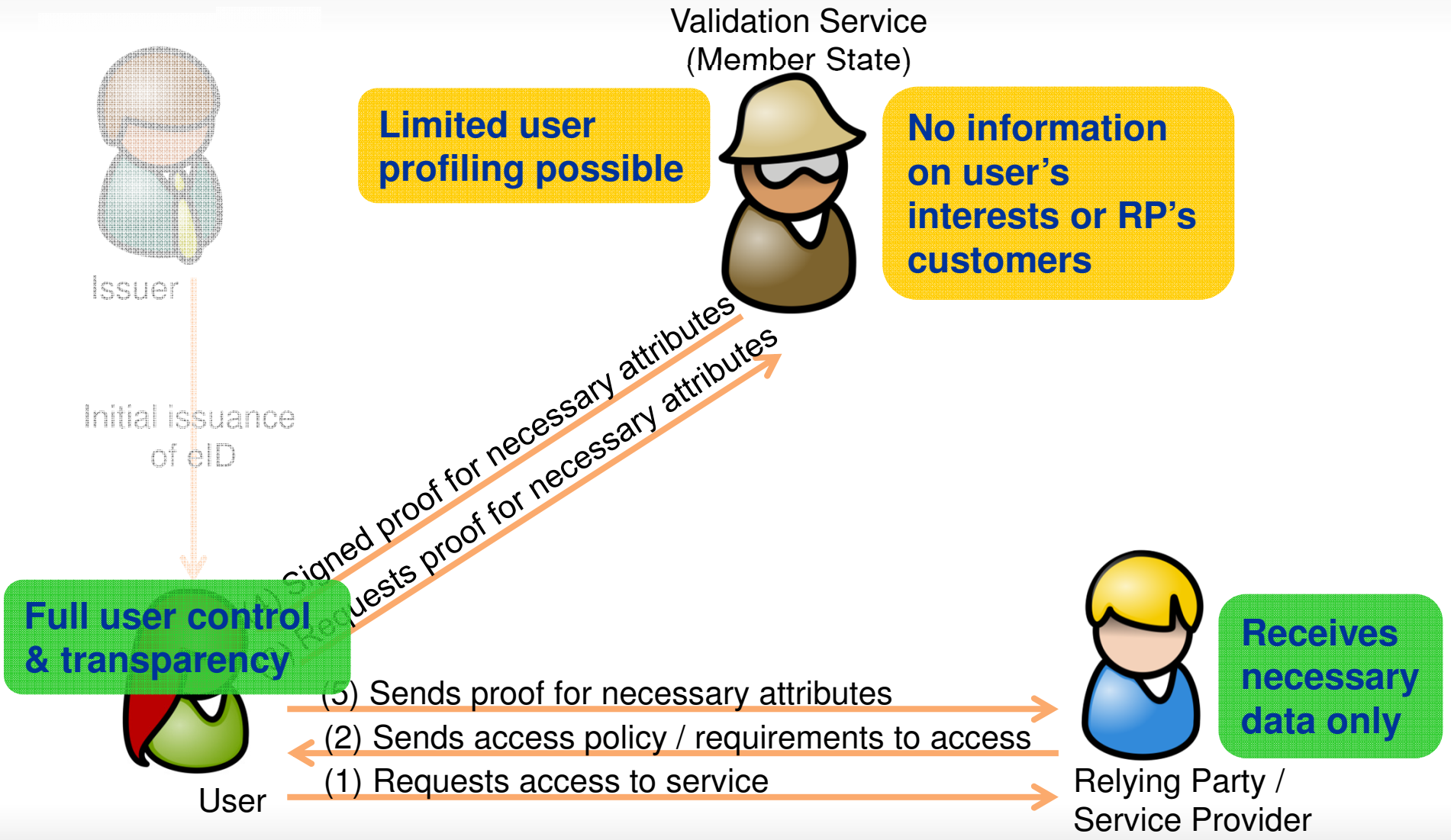
Current draft Art. 6 (1) (d) eIDAS



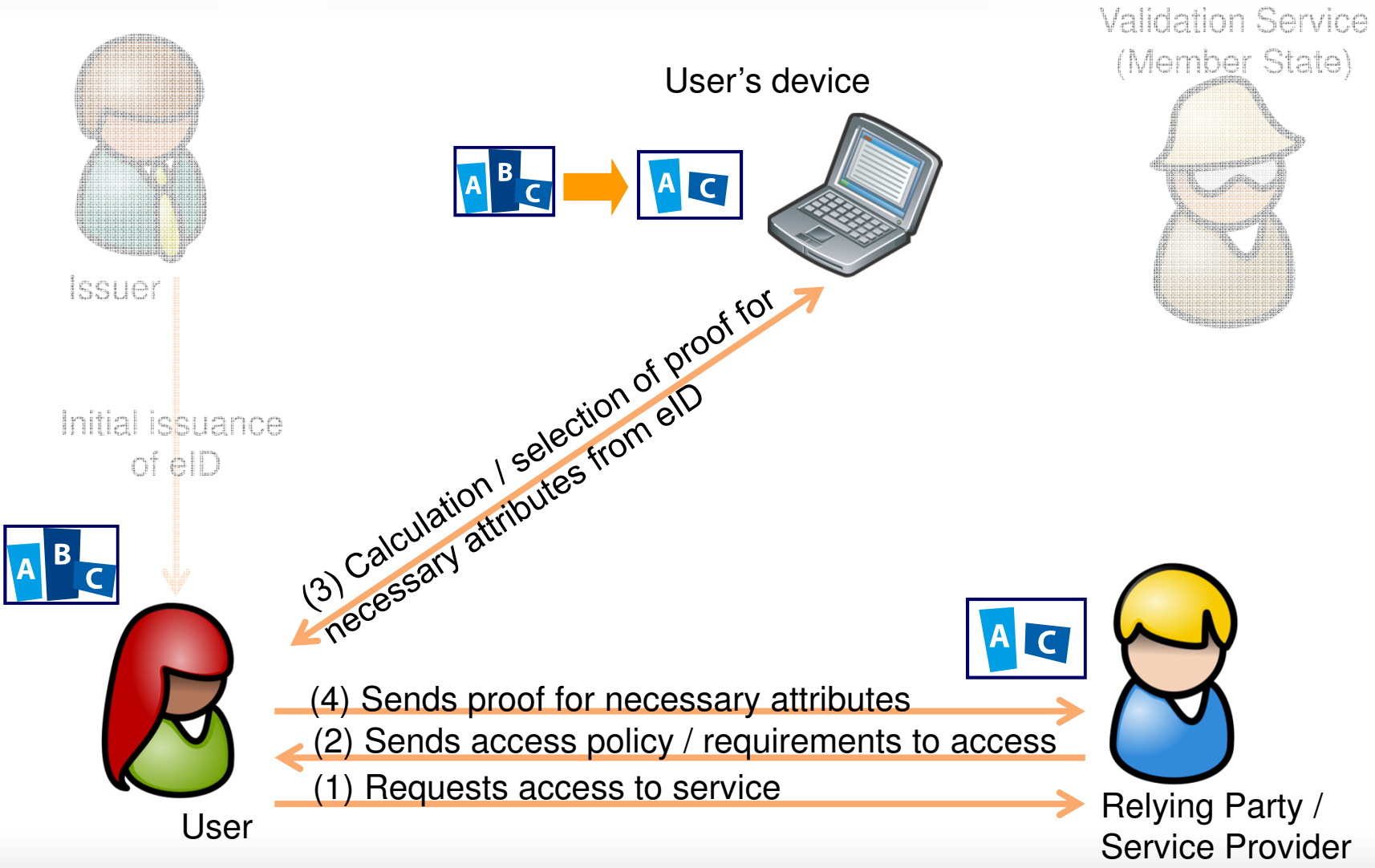
Validation Service as privacy enabler



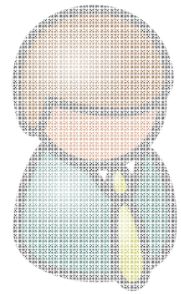
Validation Service as privacy enabler



Best practice solution with Privacy-ABCs



Best practice solution with Privacy-ABCs



Issuer

Initial issuance of eID

User's trust domain

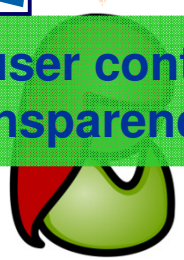
User's device

Validation Service not necessary

Profiling impossible

(3) Calculation / selection of proof for necessary attributes from eID

Full user control & transparency

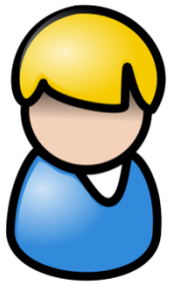


User

(4) Sends proof for necessary attributes

(2) Sends access policy / requirements to access

(1) Requests access to service



Relying Party / Service Provider

Receives necessary data only

Necessary privacy adjustments to the draft eIDAS regulation

III. Data protection for eID chapter

- Current draft references data protection only for Trust Services
- Clarify that data protection applies also to Issuers and Validation Services by moving reference to chapter I
- Especially: Regulate retention of personal data for Validation Services

Summary

I. Emphasize concept of authentication instead of identification

II. Remove barriers for privacy-preserving solutions

III. Data protection for eID chapter

Thank you for your attention

ABC4Trust Position Paper

Privacy-ABCs and the eID Regulation

ABC4TRUST

The next generation of eIDs could bring strong and efficient data protection to European citizens with Privacy-preserving Attribute-based Credentials (Privacy-ABCs). In particular, the feature enabling users to just verify individual attributes instead of sending the complete set of identifying information is a leap for data protection.
However, the current wording of the draft Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (COM/2012/238, hereinafter: eIDR) would hinder the deployment of advanced privacy features. It thereby fails its aim to be technology neutral. The eID Regulation also disregards the data minimisation principle. Besides this, the architecture logically following from the proposal requires one or more centralised national online authentication services which could profile their users' behaviour.

The attribute selection feature

The currently used eID solutions in Europe are mainly based on the principle of clearly identifying a person. Likewise, existing authentication methods in the ICT area which are based on signed certificates containing the attributes of the user (e.g. X.509) aim at identifying entities with all attribute values contained in the certificate. Any usage of such an eID or certificate may expose a lot of identity information of the holder (e.g. name and age) to the party requesting the authentication for a specific purpose. But there are various scenarios where the user of such certificates unnecessarily reveals more information than needed. E.g. if proof is required that the user is of a given age, living within a certain municipality, region or country, is a student of a university or a pensioner, neither the identity nor the exact birth date needs to be known by the other party. Revealing more information than necessary not only harms the privacy of the users, but also increases the risk of information abuse (e.g. identity fraud) and furthermore enables linkability of the user's behaviour across domains. Processing more data than necessary also violates the principle of proportionality laid down inter alia in Art. 6 sec. 1 lit. c) and e) of the EU Data Protection Directive 95/64/EC.
Advanced eID and authentication schemes allow users to securely verify individual attributes and proofs over selected attributes (selective disclosure). Privacy-ABCs enable users to provide values of individual attributes instead of sending a whole set of identifying information. So, only revealing the place of living or the birthdate is possible. Also, calculations over such attributes can be done such as the verification that the birthdate is at least 18 years before the current date or that a person lives within municipality A, B, C or D without revealing the municipality. Beyond the current scope of eIDs used in eGovernment, banking or healthcare Privacy-ABCs are not limited to certain attributes, allowing e.g. to verify that one has a certain academic degree, is advocate, member of a group or similar. At this point, other schemas offering attribute selection such as the German federal eID ("neuer Personalausweis", nPA) fall short, but should nevertheless be mentioned as a privacy-preserving solution.

Scope of the eID Regulation

The draft of the eID Regulation serves the positive and useful purpose to remove barriers in the internal market for certain electronic interactions. For this, a Member State may notify an electronic identification scheme which it accepts itself to access public services demanding an electronic authentication (eGovernment). All Members States must recognise and accept foreign notified schemes for their own eGovernment applications. While the mandatory recognition of eIDs does not oblige service providers in the private sector to recognize foreign eIDs, the regulation clearly intends to set the stage for private services, cf. Recital 14 eIR. Therefore it will have a stronger long-term impact on the eID market than the narrow field of application may suggest at first sight. So it must be carefully tailored to data protection requirements, and be open for necessary adaptations to preserve privacy in the long term.
Besides eIDs the regulation also addresses trust services which are not object of this position paper.

Cornerstones of the eID Regulation

The Regulation of eIDs follows a series of central aims: From its wording and setup, the Regulation focuses on identification of individuals in the sense of an unambiguous link to a person, and Member States are liable for the unambiguity of the link, cf. Art. 6 (1) (c) and (e) eIDR.
The draft follows the approach to be technology neutral to avoid precluding any of the existing or emerging eID technologies. Member States must further ensure the availability of an online authentication service for their notified eID schemes. They may not impose any specific technical requirements on relying parties, cf. Art. 6 sec. 1 lit. d) eIDR. This excludes any requirements for relying parties to obtain specific hardware or software, cf. Recital 15 eIDR.

Data protection in the Regulation

Art. 11 eIDR already contains specific data protection requirements that are in line with the European Data Protection Directive 95/46/EC. However, this Article does not refer to the entities responsible for the provisioning of eIDs. As those entities collect data for the verification of the link to the natural or legal person to be identified later the applicability of data protection requirements should be clearly stipulated in this draft Regulation. The positioning of Art. 11 eIDR in Chapter III "Trust Services" further suggests that it does not apply to national authentication services. A clarification is necessary that authentication services are trust services in the sense of the Regulation and thus have to comply with all requirements in Chapter III including data protection.

Figure 1: Pillars of the eID Regulation contradicting Privacy and technological neutrality

ABC4Trust position paper

Questions? Comments?

Contact:
Harald Zwingelberg
abc4trust@datenschutzzentrum.de
www.datenschutzzentrum.de
+49 (0)431 / 988-1200

Further information:
ABC4Trust research results are published at: www.abc4trust.eu