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
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
• Order alcohol online? Data to provide:

Status of many current eID solutions
Attribute Selection

• Order alcohol online? Necessary data:

- Over 18
- Valid eID
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 is fixed on architecture with Relying Party talking to Validation Service:

Art. 6 (1) (d) eIDAS: “… the notifying Member State ensures the availability of an authentication possibility online, at any time and free of charge so that any relying party can validate the person identification data received in electronic form.”

1. Requests access to service
2. Sends access policy / requirements to access
3. Sends person identification data in el. form

Issuer

Validation Service (Member State)

User

Relying Party / Service Provider
Initial issuance of eID

Validation Service (Member State)

(1) Requests access to service
(2) Sends access policy / requirements to access
(3) Sends person identification data in el. form
(4) Sends ID data
(5) Validates ID data

User

Relying Party / Service Provider
Current draft Art. 6 (1) (d) eIDAS

1. Requests access to service
2. Sends access policy / requirements to access
3. Sends person identification data in el. form
4. Sends ID data
5. Validates ID data

Validation Service (Member State)

Learns about RP’s customers

Profiling of users possible

Gains full set of ID data

Initial issuance of eID

No transparency
No user control

Issuer

User

Relying Party / Service Provider
Validation Service as privacy enabler

Validation Service (Member State)

1. Requests access to service
2. Sends access policy / requirements to access
3. Requests proof for necessary attributes
4. Sends proof for necessary attributes
5. Sends proof for necessary attributes

Initial issuance of eID

User

Issuer

Relying Party / Service Provider
Validation Service as privacy enabler

Issuer

Initial issuance of eID

Full user control & transparency

User

Validation Service (Member State)

Limited user profiling possible

No information on user’s interests or RP’s customers

Relying Party / Service Provider

Receives necessary data only

(1) Requests access to service

(2) Sends access policy / requirements to access

(3) Sends proof for necessary attributes

(4) Requests proof for necessary attributes

Limited user profiling possible

No information on user’s interests or RP’s customers

Full user control & transparency

User

Limited user profiling possible

No information on user’s interests or RP’s customers

Full user control & transparency

Received necessary data only

Relying Party / Service Provider

(0) Validates proof for necessary attributes

(1) Requests access to service

(2) Sends access policy / requirements to access

(3) Sends proof for necessary attributes

(4) Requests proof for necessary attributes

(5) Sends proof for necessary attributes
Best practice solution with Privacy-ABCs

1. Requests access to service
2. Sends access policy / requirements to access
3. Calculation / selection of proof for necessary attributes from eID
4. Sends proof for necessary attributes

Issuer

User's device

Validation Service
(Member State)

Initial issuance of eID

User

Relying Party / Service Provider
Best practice solution with Privacy-ABCs

Issuer

User Relying Party / Service Provider

Validation Service (Member State)

Initial issuance of eID

Requests access to service

(2) Sends access policy / requirements to access

(1) Requests access to service

User’s trust domain

User’s device

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

Best practice solution with Privacy-ABCs

Privacy-ABCs

User’s device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User

Full user control & transparency

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

(4) Sends proof for necessary attributes

Receives necessary data only

User's device

User
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
The next generation of eDIs could bring strong and efficient data protection to European citizens with Privacy-preserving Attribute-based Credentials (Privacy-ABCs) allowing so-called "zero-knowledge proving" without revealing the complete set of identifying information as a key for data protection.

However, the current wording of the draft Regulation on Electronic Identity Services (eIDAS) would hinder the deployment of advanced privacy features. It thereby fails to fully exploit the potential of the eID Regulation when developing the data protection services. Moreover, this is the architecture logically following from the proposal requires one or more centralized online authentication services which would violate these privacy features.

The attribute selection feature

The currently used eID solutions in Europe are mainly based on the principle of directly identifying a person. However, existing authentication methods in the ICT area which are based on signed certificates containing the attributes of the user (e.g. fingerprint, face, iris, voice) generally provide only limited privacy and attribute selection. As a result, the selection of attributes combined in the certificate can expose a lot of identity information of the holder (e.g., name and age).

In contrast, the attribute selection feature allows for making a subset of the attribute values contained in the certificate available. This feature can be used to protect privacy of the user in certain situations. For example, if a user wants to access a certain service, he/she can select only the attributes that are necessary for this purpose. But there are even cases where the user of such certificates unnecessarily reveals more information than needed. E.g. a proof of identity is required when opening a bank account within a certain municipality, whereas a certificate containing the user's full name and address is a means of a longlasting privacy violation regardless of the user's behavior across domains. Providing more information than necessary only exposes the individual to a higher risk of identity theft.

ABC4Trust Position Paper

Privacy-ABCs and the eID Regulation

The next generation of eDIs could bring strong and efficient data protection to European citizens with Privacy-preserving Attribute-based Credentials (Privacy-ABCs) allowing so-called “zero-knowledge proving” without revealing the complete set of identifying information as a key for data protection.

However, the current wording of the draft Regulation on Electronic Identity Services (eIDAS) would hinder the deployment of advanced privacy features. It thereby fails to fully exploit the potential of the eID Regulation when developing the data protection services. Moreover, this is the architecture logically following from the proposal requires one or more centralized online authentication services which would violate these privacy features.

The attribute selection feature

The currently used eID solutions in Europe are mainly based on the principle of directly identifying a person. However, existing authentication methods in the ICT area which are based on signed certificates containing the attributes of the user (e.g. fingerprint, face, iris, voice) generally provide only limited privacy and attribute selection. As a result, the selection of attributes combined in the certificate can expose a lot of identity information of the holder (e.g., name and age). In contrast, the attribute selection feature allows for making a subset of the attribute values contained in the certificate available. This feature can be used to protect privacy of the user in certain situations. For example, if a user wants to access a certain service, he/she can select only the attributes that are necessary for this purpose. But there are even cases where the user of such certificates unnecessarily reveals more information than needed. E.g. a proof of identity is required when opening a bank account within a certain municipality, whereas a certificate containing the user’s full name and address is a means of a longlasting privacy violation regardless of the user’s behavior across domains. Providing more information than necessary only exposes the individual to a higher risk of identity theft.

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