ABC4Trust
Position on the eIDAS Regulation

The next generation of eIDs could bring strong and efficient data protection to European citizens with Privacy-enhancing 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 Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and repealing Directive 1999/93/EC (hereinafter: eIDAS Regulation) might hinder the deployment of advanced privacy features. It thereby is in danger of missing its target to be technology neutral. The architecture logically following from the eIDAS Regulation requires one or more centralised national online authentication services which could profile the eID usage of the citizens. In order to reach the goal of being compliant with Directive 95/46/EC – including the data minimisation principle – and facilitating the principle of privacy by design the authentication services should be able to minimise the data which is transferred.

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 date of birth 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 (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 date of birth is possible. Also, calculations over such attributes can be done such as the verification that the date of birth 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 eIDAS 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 Member 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 recognise foreign eIDs, the Regulation clearly intends to set the stage for private services, cf. Recital 17 eIDAS. 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, when putting the Regulation into practice the data protection requirements need to be watched carefully. To preserve privacy in the long term, some clarifications of the legal text would be useful.
Besides eIDs the Regulation also addresses trust services which are not object of this position paper.

Cornerstones of the eIDAS 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. 7 (1) d) and e) eIDAS.
It follows the approach to be technology neutral to avoid precluding any of the existing or emerging eID technologies, cf. Art. 12 (3) lit. a).
Member States must further ensure the availability of an online authentication service for their notified eID schemes. They shall not impose any specific disproportionate technical requirements on relying parties, cf. Art. 7 (1) lit. f) eIDAS. The Regulation "calls" for the Member States not to impose any requirements for relying parties to obtain specific hardware or software, cf. Recitals 19, 23 eIDAS.

Data protection in the Regulation

Art. 5 eIDAS stipulates that the processing of personal data shall be carried out in accordance with the European Data Protection Directive 95/46/EC. As it is located in Chapter I "General Provisions", it applies to all subsequent sections and thus also to the entities responsible for the provisioning of national eIDs who process data for the verification of the link to the natural person to be identified later (national authentication services). Furthermore, Art. 12 (1) lit. c) eIDAS determines that the interoperability framework, so to say the "connection" between the respective notified national identification schemes, shall facilitate the implementation of the principle of **privacy by design**. Art. 12 (1) d) eIDAS stipulates that the processing of personal data within the framework needs to be carried out in accordance with the DPD. Compared to the EC's original draft this wording is a step forward as it clarifies that data protection rules need to be regarded (also) with respect to authentication services. Concerning data protection the original draft did only refer to trust services.

Data protection uncertainties

Although some gaps were closed, the eIDAS Regulation still has a series of uncertainties in the area of data protection as well as in user-centric and self-determined identity management.
To provide the required national online authentication service that does not require specific hardware or software, the most obvious solution would be to set up one or several centralised services by the notifying Member State. Due to its function as a "gateway", such a service would gain knowledge of the identifying attributes of the citizen which it must authenticate.
To retain evidence in case of liability requests for inaccurate ID information

ABC4Trust
Position on the eIDAS Regulation

(Art. 11 eIDAS), such a service is likely to create and store log entries of the authentication process. This information allows to **monitor and profile** the citizens concerned. If the relying party also identifies itself, user interests and communication behaviour additionally enrich the profiles gained.

The focus on identification and the requirement that the link to the person must be unambiguous together with the centralised verification architecture makes it hard to imagine solutions allowing authentication only with the attributes necessary for the transaction (see the attribute selection section above) or enable pseudonymous uses. It may even be hard to omit the transfer of unnecessary attributes such as the exact date of birth if only the name and address is necessary. In order to ensure the observation of **the data minimisation principle,** an authentication service should be able to verify individual attributes or derived values. The possibility to implement such a functionality is not excluded by the eIDAS Regulation, but implied neither and therefore may be overlooked. While this does not solve the risk of profiling by authentication services, it would be a major step towards data protection and may trigger further considerations to stop processing unnecessary attribute values. It would also partly preserve the advantages of privacy-preserving eID solutions such as the German nPA.

The eIDAS Regulation states in its Recitals 19, 23 and 56 that national electronic identification schemes should not impose hard- or software requirements and related costs on the other Member States. Ruling out any specific hardware or software requirements for relying parties accessing the national authentication services would factually ban advanced authentication solutions such as Privacy-ABCs or the German eID. If the interoperability framework really is meant to facilitate the implementation of the principle of privacy by design, the Regulation may not ban privacy-enhancing techniques due to their technical requirements. To fully function and provide their potential to enhance data protection inter alia by omitting a central party, Privacy-ABCs depend at least on software to be deployed by the relying party. In this respect the eIDAS Regulation **falls short behind its aim to ensure technological neutrality**. The ban of additional requirements for relying parties is understandable in the light of the mandatory mutual recognition and acceptance and the consequently following necessity to deploy and maintain such installations at all eGovernment services in Europe. However, it needs to be balanced in a way that reasonable efforts may be required to preserve the advantages of privacy-preserving solutions that exist (German nPA) or may be deployed broader in the future such as Privacy-ABCs. Reasonable efforts to prevent a **technological lock-in** may include the installation and maintenance of software that is available free of charge from the Member State notifying the eID scheme and that is easy to deploy such as browser plug-ins for user clients or a complete image to run a virtual machine at a central component of the relying parties' infrastructure.

Use cases in eGovernment

An argument brought forward in favour of the current principle of "technological neutrality" and against systems supporting selective disclosure had been a lack of use cases in the area of eGovernment. This misses that in particular processes necessary for **direct democracy** and enhanced participation rights could tremendously benefit from anonymous authentication. Petitions, polls, votings below the level of elections, and party-internal forming of opinions would profit from these possibilities. Privacy-ABCs support setting rules flexible for different use cases such as allowing each person only to attend once or to cast up to 3 votes but not for the same person etc. The ability to engage oneself politically without the need to identify oneself could get persons involved in civil rights discussions that are currently frightened off by potential negative reactions of the government or the public – e.g. in the area of equality for same-sex partnerships, religious or ethnic minorities, or for announcing public demonstrations. This way direct democratic decisions and civil rights can be strengthened in the governmental sector – Privacy-ABCs would ensure the necessary level of non-linkability for the protection of citizens.

Given our basic assumption that the Regulation directly influences the eID landscape and consequently also will be used by the private sector, the line of argumentation should not be limited to eGovernment.

Suggestions

By stipulating that all processing of personal data shall be carried out in accordance with the Data Protection Directive 95/46/EC (Art. 5 (1) eIDAS), services are obliged to adopt state-of-the-art security and privacy technologies (cf. Art. 17 95/46/EC).This also can be derived from Art. 12 (3) lit. c), facilitating the principle of privacy by design. To actually be able to follow the technical development and to ensure technological neutrality, the architecture following inherently from the eIDAS Regulation must be open for alternative approaches. Implementing the Regulation in a privacy-preserving way is not excluded by the actual legal text. However, to ensure an appropriate interpretation, the meaning of security and privacy should be emphasized, for instance by not only demanding the facilitation of privacy by design, but fostering it through clarifications in the upcoming implementing acts.

ABC4Trust at a glance

Project reference:

257782

Project duration:

November 2010 – February 2015

Partners:

12 partners from industry, academia, research centres and data protection authorities

Costs:

€ 13.59 Million (€ 8.85 Million EU funded)

Funding:

The ABC4Trust project receives research funding from the European Union's Seventh Framework Programme under grant agreement n°257782 as part of the "ICT Trust and Security Research" theme.

Project coordination:

Prof. Dr. Kai Rannenberg
Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt am Main
Grüneburgplatz 1
60629 Frankfurt am Main
Germany
contact@abc4trust.eu

Contact:

Marit Hansen
t: +49 431 988 1214
f: +49 431 988 1223
press@abc4trust.eu

Version and date of publication:

Version 2.0, December 2014

Want more info?

https://abc4trust.eu/

SEVENTH FRAMEWORK PROGRAMME