Source: **Marko Hölbl**
CEPIS LSI SIN

Version: **v1.3./2.4.2015**

Document for:

Decision	x
Discussion	
Information	
Publication	

Position on the Electronic identification and trust services (eIDAS)

CEPIS

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote a high standard among Informatics Professionals in recognition of the impact that Informatics has on employment, business and society. CEPIS – which represents 33 Member Societies in 32 countries across greater Europe – has agreed on the following statement:

1. Background

According to the Digital Agenda for Europe[i] Electronic identification (eID) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market.

On July 23, 2014 a new Regulation on electronic identification and trust services for electronic transactions in the internal market (hereafter: the eIDAS Regulation) was adopted by the European Parliament and the Council. This Regulation aims to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens, and public authorities. It is intended to increase the effectiveness of public and private online services, eBusiness, and electronic commerce in the EU. All implementing acts by the European Commission (secondary legislation) are to be completed in September 2015. However, the Regulation will not enter fully into force before July 2016.

More specifically the eIDAS Regulation aims to deliver a predictable regulatory environment related to electronic identification and trust services. The goal of this regulatory environment is to encourage user convenience, trust, and confidence in the digital world, while keeping pace with technological developments, promoting innovation,

and stimulating competition[ii]. Therefore all Member States must recognise and accept foreign notified schemes for their own eGovernment applications. In this sense the regulation is clear regarding eGovernment, but does not apply to service providers in the private sector. Mandatory recognition of eIDs does not oblige service providers in the private sector to recognise foreign eIDs. However, the regulation clearly intends to set the stage for private services, too, as it encourages the private sector to voluntarily use identification means under a notified scheme for identification purposes (Recital 17 eIDAS Regulation).

The eIDAS Regulation follows a series of central aims. From its wording and setup, the regulation focuses on authentication of individuals in the sense of an unambiguous link to a person, and Member States are liable for the unambiguity of that link[iii]. 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[iv]. The eIDAS Regulation requests that Member States not impose any requirements for relying parties to obtain specific hardware or software[v]. Art. 5 of the eIDAS Regulation stipulates that the processing of personal data shall be carried out in accordance with the European Data Protection Directive[vi].

The eIDAS Regulation will have a stronger long-term impact on the eID market than the narrow field of application may suggest. Therefore, when putting the regulation into practice, data protection requirements need to be carefully observed. In particular, the eID solutions currently used in Europe are mainly based on the principle of **identifying a person uniquely**. In order to reach the goal of being compliant with the EU Data Protection Directive **including its data minimisation principle,** and to facilitate the principle of privacy by design, the authentication services should be able to minimise the data which is transferred.

2. Concerns

Given the current state and wording of the eIDAS Regulation, it may hinder the deployment of advanced privacy features. The architecture logically following from the eIDAS regulation presumes one or more centralised national online authentication services. Namely, in order to provide the required national online authentication service ("interoperability framework"), one which does not require the relying parties to have specific hardware or software, the most obvious solution would be for the notifying Member State to set up one or several centralised services. 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, such a service is likely to create and store log entries of the authentication process. This information allows monitoring and profiling the respective citizens. If the relying party also identifies itself, user interests and communication behaviour additionally enrich the profiles gained. The issue can be illustrated by an analogy to physical identification cards (IDs), which are a common means of identification in several EU Member States. In such a scenario, the authentication of a person is conducted in an "off-line manner", e.g. when a person checks in to a hotel. The verifier (or relying party) does not need to contact anyone when checking the ID. The idea of having to call the issuer of the ID each time, when

checking it, e.g. calling the issuer each time, when a traveller checks in at a hotel would not match a free society, as it would generate a traveller and hotel track record at the ID issuer, Consequentially the same tracking or getting additional information about a person or institution should also be avoided in the online world.

The focus on identification and the requirement that the link to the person be unambiguous, together with the centralised verification architecture, makes it hard to imagine solutions that allow authentication with only the attributes necessary for the transaction or that enable pseudonymous use. It may e.g. 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 of implementing such functionality is not excluded by the eIDAS Regulation, but neither is it implied and therefore may be overlooked.

For example, existing authentication methods in the ICT area, based on signed certificates containing the attributes of the user, 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 the holder's identity information (e.g. name, age) to the party requesting the authentication for a specific purpose. But there are various scenarios where the user unnecessarily reveals more information than needed. For example, 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 name nor the exact date of birth needs to be known by the relying party. Revealing more information than necessary not only harms the privacy of users, but also increases the risk of information abuse and furthermore enables linkability of the user's behaviour across domains. Processing more data than necessary also violates the principle of proportionality as to the EU Data Protection Directive.

While transferring only the attributes necessary for the transaction 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 eID[vii].

As another example, the eIDAS Regulation states that national electronic identification schemes should not impose hard or software requirements and related costs on the other Member States. However, ruling out any specific hardware or software requirements would factually ban advanced authentication solutions such as Privacy-ABCs[viii] or the German eID[ix]. Privacy-preserving Attribute-based Credentials (Privacy-ABCs) is a technique offering authentication and a high level of security to service providers, while preserving users' privacy. The technology enables users to obtain credentials containing certified attributes and later derive unlinkable tokens that only reveal the necessary subset of information needed by the service provider[x].

Therefore in this case, the principle of "technological neutrality" has raised challenges regarding implementation, which need to be addressed. In particular, processes necessary for direct democracy and enhanced participation rights could tremendously benefit from such privacy enablers as anonymous authentication. Petitions, polls, voting below the level

of elections, and party-internal opinion formation would benefit from these possibilities. The ability to engage oneself politically without the need to identify oneself could involve people in civil rights discussions that they are currently frightened of engaging in due to potential negative reactions from the government or the public, e.g. in the area of equality for same-sex partnerships, religious or ethnic minorities.

3. Recommendations

The next generation of eIDs could bring strong and efficient data protection to European citizens. In the electronic identification and trust services environment for electronic transactions, the realization of identification and authentication using an eID should prevent tracking of users.

One of the possible technologies is thus Privacy-preserving Attribute-Based Credentials (Privacy-ABCs). In particular, the feature enabling users to only verify individual attributes instead of sending the complete set of identifying information is a leap forward for data protection.

To actually be able to follow the technical development and to ensure technological neutrality, the architecture following inherently from the eIDAS Regulation should be open to alternative approaches. Therefore, to ensure an appropriate interpretation, it is recommended that the meaning of security and privacy be emphasised, for instance by not only demanding the facilitation of privacy by design, but also fostering it through clarifications in the upcoming implementing acts. To preserve privacy in the long term, some clarifications of the legal text would be useful.

References

[i] Digital Agenda for Europe, Trust Services and eID, http://ec.europa.eu/digital-agenda/en/trust-services-and-eid, last visited on 28/3/2015.
[ii] Electronic identification and trust services (eIDAS): regulatory environment and beyond - European Commission, http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond, last time visited: 28/3/2015
[iii] cf. Art. 7 sub d) and e) of the eIDAS Regulation.
[iv] cf. Art. 7 sub. f) of the eIDAS Regulation.
[v] cf. Recitals. 19 and 23 of the eIDAS Regulation.
[vi] 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, COM/95/375 COM/92/422 COM/90/314-2; see: http://eur-lex.europa.eu/legal-content/en/NOT/?uri=CELEX:31995L0046
[vii] The German National Identity Card, http://www.personalausweisportal.de/EN/Home/home_node.html, last time visited: 28/3/2015
[viii] ABC4Trust: Attribute-based Credentials for Trust, http://abc4trust.eu/, last time visited: 28/3/2015
[ix] The German National Identity Card, http://www.personalausweisportal.de/EN/Home/home_node.html, last time visited: 28/3/2015
[x] ABC4Trust: Attribute-based Credentials for Trust, http://abc4trust.eu/, last time visited: 28/3/2015