Principles and guidance on eID interoperability for online platforms

Background

The Commission Communication on Online Platforms and the Digital Single Market (*COM(2016)288*) states that online platforms should inform users more effectively what personal data is collected and how it is shared and used, in line with the EU data protection framework. More generally, this issue includes the ways in which users identify themselves in order to access online platforms and services.

In order to empower consumers and to safeguard the principles of competition, consumer protection and data protection, it is foreseen in the Communication that *"the Commission will further promote interoperability actions, including through issuing principles and guidance on eID interoperability at the latest by 2017. The aim will be to encourage online platforms to recognise other eID means — in particular those notified under the eIDAS Regulation (EC) 910/2014— that offer the same reassurance as their own"*.

Electronic identification *is the process of using a set of data in electronic form uniquely representing a person (natural or legal).*

Authentication *refers to an electronic process that enables the electronic identification of a natural or a legal person, or the origin and integrity of data in electronic form to be confirmed.*

Notified eID means *refers to government-issued/recognised eID means which have been notified by the Member States according to eIDAS rules as a prerequisite for mutual recognition across the EU.*

The term ***online platforms*** *should be understood in the context of the Communication on Online Platforms and the Digital Single Market and description provided therein.*

Identification of users in online platforms is often challenging. Most online platforms require users to register with their real identity. However, verifying the identity is not always easy, often requiring the use of complex tools and can be costly.

In the EU, the eIDAS Regulation introduced a predictable *legal framework for cross-border mutual recognition of secure and trustworthy electronic identification means* issued or recognised by national public authorities. These can be electronic or mobile IDs, national identity cards, bank cards and others – always based on *multi-factor authentication* as the baseline. In the EU, we also have an interoperability framework which makes the cross-border use possible.

By 29 September 2018, EU citizens and businesses will be able to use their "notified" government-issued/recognised eID means to identify/authenticate themselves when accessing online public services across the EU. In this regard, the Commission is supporting the Member States to deploy an eIDAS compatible eID interoperability infrastructure with funding and technical support under the Connecting Europe Facility (CEF) programme. The rolling out by the EU Member States of eID means to be recognised for cross-border access to public services will allow European citizens, businesses and public administrations to benefit from a trusted and legally enforceable framework for cross-border use of electronic identity means that, de facto, will contribute to establishing a true EU jurisdictional security in the digital environment.

Government-issued or recognised eID means establish the digital identity of a person (natural or legal) in a way in which a person can prove they are who they claim to be to a third party with an adequate level of assurance across Europe. They can provide trust and security not only to the public sector, but also to the private. Unless mandated by law or regulations for specific activities, it is a decision of the private sector whether or not to use such eID means and it is certainly an opportunity to be considered.

There is already ongoing collaboration with the banking/financial sector where eID and trust services may play a key role in meeting their regulatory obligations – under the Payment Services Directive 2, the Anti-Money Laundering Directive 4 (and the upcoming 5) – on security and identification related

to know-your-customer (KYC) in digital on-boarding activities, as well as strong authentication of parties to electronic payment transactions. Furthermore, in March 2017 the European Commission published an Action Plan (COM/2017/0139) setting out a strategy to strengthen the EU single market for retail financial services. The Action Plan will harness the potential of digitalisation and technological developments (FinTech) to improve consumer access to financial services across the EU.

The use of government-issued/recognised eID means can bring benefits to many sectors, including online platforms, thereby easing the digital transformation of organisations, enhancing the customer experience and stimulating the provisioning of new and innovative services. In order for this to become a reality and to fully operationalise the use of eID means under eIDAS beyond the public sector – across commercial sectors and application domains – the active involvement and collaboration of all relevant stakeholders is crucial. In this regard, the discussions related to elaboration of the current principles, as well as the setting up of a dedicated expert group in the context of the Action Plan on retail financial services, will play an important role.

Preamble

In line with the eIDAS Regulation, as of 29 September 2018, any citizen in the European Union will be able to use her or his national eID means (notified according to eIDAS rules), to identify/authenticate when accessing online public services in any other Member State. Such eID means are multi-factor and cross-border by default and correspond to a homogenous level of assurance meeting a clearly defined set of criteria.

By allowing users to freely decide whether they want to use government-issued/recognised eID means, which are at their disposal and already used in other domains, online platforms can empower users and enhance their digital experience – by providing them with extended consumer choice, while ensuring the same or a higher level of convenience, security, trust and respect of privacy and a high level of protection of personal data.

The goal of this set of principles and guidance is to facilitate online platform users, if they wish so, to rely on their own government-issued/recognised eID means whenever the access to online platforms may require electronic identification or authentication steps. In this regard, the principles and guidance aim to reflect values that everybody (users and online platform providers) can subscribe to as well as a shared understanding of how everybody can interact and exploit the full potential benefits of the eID framework in the online platform ecosystem in the future.

The principles and guidance are the result of a participatory and co-creation process involving relevant stakeholders and supported by the Commission. They are not legally binding. The overall ambition of this initiative is that, once finalised, the principles and guidance will be endorsed and respected by as many stakeholders, representing various positions, as possible – in particular online platform operators, organisations representing individual and business users, digital identity providers, etc.

Principles

Whenever online platforms require users to undergo identification or authentication steps the following principles shall apply:

User choice

Users should be allowed to decide whether to identify/authenticate themselves by relying on eID means of their choice, provided that such means meet the level of assurance required by the online platform.

Privacy

Online platform users should be able to rely upon trusted identification and authentication mechanisms of their choice, which provide them with the desired level of privacy.

Interoperability and Security

Government-issued/recognised eID means, that are multi-factor by default and provide a homogenous level of assurance equal to or higher than the level required for the identification/authentication step, should be regarded as an appropriate tool to safely enrol users, quickly validate their identity, and minimise security risks.

Trust

Online platform users should have the freedom to rely upon the secure authentication means of their choice which they trust most in the context of a particular transaction. Such trust should be based on full transparency and user awareness about the relevant data privacy and security implications.

Convenience

Online platform operators should ensure that the user experience and convenience of identification/authentication processes relying upon government-issued/recognised eID means – in terms of speed, ease of use and seamlessness – is not diminished compared to other identification/authentication methods.

User consent and control

Users should be able to exercise control over the data which are being exchanged for the purposes of identification/authentication and to selectively disclose only those attributes that are required for a particular transaction.

Proportionality

The request for personal information by online platform operators to the eID service should be minimal, proportionate and contain only the information relevant to the particular transaction.

Know your counterpart

As a way of enhancing mutual trust between counterparts in a transaction, whenever the identity of a user had been duly verified via government-issued or other legally enforceable eID means, this should be indicated in the user profile.

Global scalability

To the extent possible, a federated eID interoperability model of government-issued/recognised eID means based on transparent and comparable assurance levels and security, should be applied and promoted on a global level.

Guidance

The following guidance is an attempt to further clarify the principles proposed above, and translate them into more concrete and operational actions. These actions are indicative, non-binding and do not aspire to be exhaustive. Their intention is to help actors to better understand and implement the principles.

- When relying upon government-issued/recognised eID means, users should not be required to provide additional detailed personal identification data in to identify/authenticate to online platforms. Such eID means should be regarded as a reliable and sufficient means for establishing a verifiable link between a digital identity and the real person behind it.
- Users should be able to preserve a level of privacy and anonymity, e.g. by using a pseudonym (already guaranteed under eIDAS – ref. to art 5.2) and/or other privacy-by-design mechanisms, associated in a trustworthy manner to their government-issued/recognised eID. This would allow providing a minimum of personal information, while maintaining the accountability, enforceability and liability for particular actions.
- Personal data exchanged for the purpose of identification/authentication to an online platform should be used in a transparent way. It should not be used for secondary, unconnected purposes without the user's informed consent.
- Users should be duly informed about the privacy implications associated to a particular identification/authentication method.
- To minimise the risk of compromised personal information, as a rule, person identification data need not be collected or stored by the platform operator. Verification of the claimed identity should be sufficient.
- Any personal information obtained by online platforms during the process of identification/authentication via government-issued/recognised eID means should be protected from improper use by default.
- When choosing an identification/authentication method, the users should be informed who has the responsibility of ensuring the security of their personal data (i.e. the platform operator or the identity provider).
- Users should always be informed on how to securely use government-issued or other legally enforceable eID means to identify/authenticate to online platforms.
- The use of government-issued/recognised eID means should remove the need for the user to repeatedly type in the same personal data for each account that he or she creates. The user should be able to share with the platform operator, in a convenient and transparent manner, relevant attributes related to the eID means of his or her choice.
- User consent on the attributes to be shared with the platform operator should be explicit. It should be requested and obtained before the actual collection of data takes place.
- Online platform operators should duly justify the need to collect certain attributes in view of the type of transaction and the level of risk. The disclosure of attributes should be transaction-specific, i.e. limited to elements that are relevant only to the specific use case, and not to the whole service portfolio of the provider.
- Online platform operators should provide, early in the process, a clear distinction between which data is mandatory and which is optional.

- The user should be duly informed if any personal data about him is stored in the context of a transaction. No authentication-related data should be stored.
- Online platform operators are encouraged to define thresholds for the information that needs to be collected from the user for the different types of transactions.
- Users should enjoy profile portability and interoperability, allowing for separating the data from the application and the user should have the right to decide where to store the data.
- Users should have the right to inspect, download and permanently delete all data related to an eID.
- Online platform operators should provide dispute resolution procedures, related to any aspect of the provision of their services, that assures the users' right to identify themselves with an eID and be bound to the applicable laws and regulations.
- Online platform operators should provide their users with information on whether their counterpart in a transaction has verified their identity by using government-issued/recognised eID means.
- Appropriate eID scheme mapping, certification and standards may be agreed, using an inclusive stakeholder approach, in order to ensure the trust chain beyond the EU Member States.