Principles and guidance on eID interoperability for online platforms

Revised draft version of January 2018

DRAFT

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 (eID) *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.*

In the specific context of these principles and guidance, ***eID means*** *refers to any mechanism that allows online platform users to both identify and authenticate electronically.*

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 and authentication of users in online platforms is often challenging. Most online platforms require users to register with their real identity. However, authenticating 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

DRAFT

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 revised Anti-Money Laundering Directive (AML) which has recently reached the political agreement by the co-legislators– 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, on 14 December 2017 the European Commission adopted a Decision setting up an expert group on electronic identification and remote Know-Your-Customer processes. Building on the Consumer Financial Services' Action Plan (COM/2017/0139) and in line with the AML rules, as of Spring 2018, the expert group will explore how to facilitate the cross-border use of electronic identification (eID) and Know-Your-Customer (KYC) portability based on identification and authentication tools under eIDAS to enable financial institutions to identify customers digitally for on-boarding purposes.

The use of government-issued/recognised eID means can indeed 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.

DRAFT

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 online platform users ("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 these principles and guidance on eID interoperability for online platform to allow and facilitate online platforms 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.

The ambition of these principles and guidance is to reflect values that everybody (users and online platforms) can subscribe to as well as a common understanding of how everybody can leverage and benefit from the possible use of trusted eID, like those recognised under eIDAS, whenever an identification or authentication step is needed to access online platform services.

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 and should always be applied in compliance with existing applicable legislation. 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 platforms, organisations representing individual and business users, digital identity providers, etc.

DRAFT

Principles

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

User awareness

Whenever an identification/authentication step is required to access a service provided or facilitated by the online platform, online platforms should make users aware of the available options concerning the use of eID means for such identification/authentication.

User choice

Online platforms should allow users to decide whether to identify/authenticate themselves by relying on the eID means of their choice, provided that such means meet the level of assurance required by the service provider or relying party involved in the transaction performed through the online platform.

Privacy

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

Interoperability and Security

Interoperable government-issued/recognised eID means should be regarded as an appropriate tool for online platforms to safely enrol users, quickly validate their identity, and minimise security risks.

Trust

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 privacy, data protection and security implications.

Convenience

Online platforms 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 personal data which are being processed for the purposes of identification/authentication or for fulfilling online platforms' legal requirements, and to selectively provide only those minimum attributes that are required for a particular transaction.

Proportionality

The request for personal information by online platforms to the eID service should be minimal, proportionate and contain only the information relevant to the particular transaction, in accordance with the applicable data protection rules, in particular the General Data Protection Regulation.

Know your counterpart

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

DRAFT

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.

DRAFT

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.

DRAFT

Guidance	Principles addressed
1. All relevant stakeholders, in particular online platforms, governments and identity providers, should collaborate in raising awareness about the use of eID means[1].	User awareness
2. Online platforms should always inform their users of the eID means available to them for accessing to their services. Whenever possible, they should also inform about how to obtain these eID means, either directly or by referencing to the entities issuing them.	User awareness
3. Identity providers should make all the information relevant for the users of the eID means available online, in particular all applicable terms, conditions and fees, including limitations of usage.	User awareness Trust
4. Online platforms should explicitly inform their users about the level of assurance required by the service provider or relying party requesting an identification/authentication through the online platform.	User choice
5. Identity providers should provide the users of their eID means with clear information about the levels of assurance corresponding to those means. In case an eID means can work according to more than one level of assurance, identity providers must inform users on how they should use the eID means for each of those levels.	User choice
6. Online platforms should facilitate user choice of the eID means by ensuring users' identification/authentication portability and interoperability, allowing for separating the data from the application and for the user to have the right to decide where to store the identification/authentication data.	User choice
7. Online platforms should facilitate users to decide what eID means to use in their services by including in their dispute resolution procedures provisions related to the users' right to identify themselves with an eID means of their choice.	User choice
8. Online platforms should duly inform their users about the privacy and data protection implications associated to a particular identification/authentication method.	Privacy Trust
9. Identity providers should make the privacy policy corresponding to the eID services they provide available online.	Privacy Trust

[1] This can be done e.g. by organising communication campaigns, producing training material.

Guidance	Principles addressed
10. Online platforms should accept users who want to preserve a high level of privacy and anonymity, e.g. by using a pseudonym (as for instance 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[2].	Privacy
11. Identity providers are encouraged to implement and offer privacy-by-design eID services that allow users to rely on trusted and enforceable anonymous credentials (such as protected digital identity tokens) which maintain a digitally un-linkable correspondence between such credentials and the related government-issued/recognised eID of the users.	Privacy
12. Identity providers of government-issued/recognised eID means should duly inform their users about responsibilities of those users regarding a safe utilisation of the eID means and how to minimise security risks.	Interoperability and security Trust
13. When choosing an identification/authentication method based on a government-issued/recognised eID means, users should be aware of the responsibilities in relation to the security of their personal data corresponding to each of the parties participating in the transaction (i.e. the platform operator, the identity provider, or the relying party).	Interoperability and security Trust
14. When relying upon government-issued/recognised eID means in order 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.	Interoperability and security
15. 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.	Interoperability and security
16. Identity providers of government-issued/recognised eID means should facilitate the acceptance of those means by online platforms by adhering to interoperability frameworks and reducing systems integration efforts (i.e. complying with widely used authentication protocols or providing APIs)	Interoperability and security
17. Identity providers of government-issued/recognised eID means should collaborate with online platforms to ensure that user experience and convenience of identification/authentication processes relying on those means matches the user experience and convenience of other identification/authentication methods.	Convenience
18. Online platforms should provide clear information on the collection of personal data and its processing in line with the EU General Data Protection Regulation principle of lawfulness of processing as set forth in Articles 13 and 14. This provision of information to individuals about the processing helps them exercise their rights (access, rectify, erase, object, portability, right not to be subject to automated-decision making).	User consent and control Trust

DRAFT

[2] This would allow providing a minimum of personal information, while maintaining the accountability, enforceability and liability for particular actions.

Guidance	Principles addressed
19. Personal data processed for the purpose of identification/authentication by an online platform should be used in a transparent and lawful way. It should not be used for secondary, unconnected purposes without the user's informed consent.	User consent and control
20. Online platforms should ask for the affirmative user consent on the attributes to be shared with the online platform when using the government-issued/recognised eID means for identification. This consent should be requested and obtained before the actual collection of data takes place.	User consent and control
21. Online platforms should, early in the process, provide a clear distinction between which data are mandatory and which are optional.	User consent and control
22. Online platform users should have the right of access, rectification, erasure and portability in relation to all personal data obtained by an online platform through the use of an eID means for the purpose of identification.	User consent and control
23. Online platforms may only disclose to service providers relying on the online platform the minimum set of personal data that is required for a particular transaction in the context of the service provided, in compliance with the applicable data protection rules. In particular, for the personal data sharing to take place, the online platforms must rely on one of the legal grounds in Article 6 of the General Data Protection Regulation and must duly inform users about such data sharing.	User consent and control
24. To minimise the risk of compromised personal information, as a rule, personal data other than the minimum set of data required for electronic identification (that is, the unique representation of a person) should not be collected or stored by the online platform. Authentication based on this minimum set of data should be sufficient ('data protection by design').	Proportionality
25. Online platforms 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 transaction, and not to the whole service portfolio of the provider.	Proportionality
26. Online platforms are encouraged to define thresholds for the information that needs to be collected from the users for the different types of transactions and inform them accordingly.	Proportionality
27. Online platforms should provide their users with information on whether their counterparts in a transaction have verified their identities in that platform by using government-issued/recognised eID means.	Know your counterpart
28. All relevant stakeholders should work towards international agreements on eID scheme mapping, certification and standards in order to ensure a trustworthy eID environment at global level.	Global scalability Interoperability and Security

DRAFT