eIDAS Policy Paper

25 January 2021

Introduction

In June 2021 the European Commission launched a reform of the 2014 eIDAS Regulation to overhaul Europe's framework for electronic identity (eID) systems.[1] This ambitious reform tries to create a counterbalance to the widespread login systems of Google, Facebook and Apple, as well as to provide widely-adopted eID systems for eGovernment and eCommerce applications to the population. Under this new draft Regulation member states would be obliged to offer a software called "European Digital Identity Wallets" (Wallet App) that allows for the online and offline identification of citizens and residents, as well as allowing them the attestation of attributes like age, driving licenses or student IDs. The draft Regulation tries to ensure the proliferation of this new European Digital Identity Wallet by forcing Very Large Online Platforms[2] like Facebook and Google to support this European Wallet as a means to log in to their services. Similarly, member states are obliged to use this system for the identification of citizens when offering eGovernment services already under the old 2014 eIDAS Regulation. Smaller internet companies can be forced by the Commission via a delegated act to also support the new Wallet App.

The following paper tries to elaborate on the biggest problems with the Commission's proposal from a privacy and digital rights perspective. A European electronic identity system needs to be respectful of fundamental rights of citizens and residents because positive potentials of this system depend on it's wide adoption and trust by all parties involved. This can only be achieved by assessing the impact this system will have on the current digital ecosystem in Europe. The current proposal leaves many core questions about the architecture open to delegated acts, which makes a comprehensive assessment almost impossible. The Regulation should clarify those points and provide proper safeguards to ensure privacy by design, user choice and data minimisation. While we accept the premise of this regulation and the need for a trusted digital identity and attestation infrastructure, not using this system should not have negative consequences for citizens that opt-out of the Wallet App or don't own a Smartphone. We hope those points can be addressed in this paper and suggested safeguards to improve the regulation will be adopted in the legislative process.

Unique, lifelong identifiers for every citizen and resident

One of the core functionalities of the Wallet App, to identify a user by exposing their legal name to a third party, is complemented in Article 11a by requiring member states to uniquely identify every person with an alphanumeric string that stays with them for the rest of their lives. This persistent and unique identifier for all European citizens and residents will be shared by the Wallet App to private and public third parties. The user still has to allow for his or her identification with an interaction on the app, but since the user very often is subject to an imbalance of power in situations of identification and this functionality is even limited to cases in which identification is required by national or European law, it can be doubted that this consent is freely given. Additionally, it is unclear how the Wallet App can distinguish between cases where identification is legally required and where it is not. Those cases can vary between member states, as for example a Hungarian law could mandate identification at demonstrations or an Austrian social media law could require Facebook to identify

1 See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A281%3AFIN&qid=1622704576563

2 This references Article 25 paragraph 1 of the draft Digital Services Act Regulation.

their users. Generally speaking, Facebook and other companies are only waiting to add such an official unique, lifelong identifier to their users' identities and will find a way to trick users into doing so. To prevent these unique, lifelong identifiers from massively helping to further increase the data-driven power of Facebook and others, they should not be created in the first place.

Suggested Solution

Deletion of Article 11a.

Proliferation of government-issued identity information and online behaviour

According to Article 6b paragraph 1 of the draft Regulation, relying parties (companies wanting their customers to use the Wallet App to identify or prove certain attributes) can request access to the European system in any member state where they are based and get a blank check to gain access for the whole EU. This allows for forum shopping as any company can pick the administration within the EU that is most favourable to them. A relying party could be any company that wants to gain access to identity information or attributes in the Wallet. The Regulation is imprecise on how exactly this verification procedure of a relying party in a member state would work. According to Article 6b paragraph 4 the Commission, via a delegated act, will decide six months after the Regulation has entered into force how this important check will happen. The Regulation offers no mechanism on how to revoke the access of a relying party from the eIDAS system. Based on the last sentence of paragraph 1 it is even unclear if the stated purpose of the processing of identity information can be considered sufficient grounds for rejecting an application.

The national eIDAS regulators are responsible for verifying that the relying party adheres to the Regulation. In the case of Ireland this is the Department of the Environment, Climate and Communications, which is not an independent regulator. The Irish Data Protection Authority is notoriously undermining European data protection law, and this risk may persist under the proposed system in eIDAS if the competent authority is not independent and accountable. The setup of the new eIDAS framework is not just falling short of the necessary safeguards for an environment that we can trust with our identity information, it is also actively repeating mistakes of the enforcement of past EU legislation, which will invite abuse of the new system by known actors.

Right now Google and other Big Tech companies that rely on targeted advertising in their business model track almost every step of our online behaviour and already profile every aspect of our lives. One of the last things they do not know with certainty in many cases is our legal name. By providing cheap and mostly unregulated access to government-certified identity information and even forcing Very Large Online Platforms to offer the Wallet App as a login method, the EU is offering on a silver plate what it should protect.

We see a high risk in the proliferation of government-certified identity information in the fields of targeted advertising, banking and financial scoring, as well as eCommerce and media. The existing shortcomings in GDPR enforcement, like prohibition of tying and pay-or-consent schemes, will amplify this problem. The eIDAS Regulation should codify proper safeguards against the misuse of identity information in the existing ecosystem it tries to address.

Suggested Solutions

In our view, the Regulation needs to be improved with safeguards against the misuse of the Wallet App by relying parties.

In light of this requirement, Article 6b needs to be amended as follows:

Relying parties should be obliged to register the concrete use case for which they want to rely on the Wallet App with the eIDAS regulator of their country that ex-ante checks it against a black- and whitelist of use cases and can also require a data protection impact assessment. Such an authorisation by one eIDAS regulator should be able to be challenged with the eIDAS regulator from another country by consumer protection and data protection organisations with the potential outcome of this use case being prohibited in that country. Examples for use cases on the blacklist are advertising, financial scoring and real name policies on social media platforms. In cases where the data protection impact assessment concluded with a high risk for the data subjects, the eIDAS regulator should be empowered to add this use case to the blacklist.

Central surveillance of every identity and attribute verification

The Wallet App aims to replace existing means of verifying identity, age and other attributes. This new system should not be worse for privacy and data protection than existing means it seeks to replace. We acknowledge that in the case of age verification a user no longer needs to hand over an ID card containing more information than necessary (name, date of birth, issuing country), which solves a specific problem. However, the proposal contains the real danger of central surveillance of every online and offline identification and attribute verification process with the Wallet App. Similar to the EU Digital Covid Certificate, the Commission would have in the proposed Regulation the power to unilaterally decide on important architectural questions via delegated act at a later stage, instead of detailing the principles of privacy by design in the legislation. We encourage the co-legislators to detail data protection, privacy and cybersecurity safeguards directly in the legislation instead of leaving it this power to the European Commission. The unobservability of all identification and attribute verification processes that are handled by the Wallet App needs to be a safeguard in the Regulation. After we raised this point during the EU Digital Covid certificate discussions[3], such a safeguard was added .[4]

There are existing self-sovereign eID systems that operate on a zero-knowledge and unlinkability paradigm, which prevents by design any centralised observation of the identification or authorisation processes. Technologies such as did:peer, DIDComm, OpenID Connect SIOP, and BBS+ Signatures[5] can be used to build privacy-preserving digital infrastructure in a way that enables the establishment and exchange of identities and attributes, without a requirement for centralised actors or blockchains. Such guarantees are missing in the Commission's proposal. The vagueness on many architectural questions of the Wallet App reinforces loopholes in the legal text of Article 6a paragraph 7 that establish a legal basis for the processing of behavioural data on the use of the Wallet App and linking this data with third parties.

The current framework allows a centralised actor to observe on a macroscopic level every identification and attribute verification in the population. For example, the Regulation allows the provider of the Wallet App (governments) to gain information on all logins at Very Large Online Platforms (Facebook, Google), on age verifications for purchasing certain goods (alcohol, tobacco, etc.) online and offline and on services for which the user only qualifies because of a certain attribute that

3 See https://en.epicenter.works/document/3425 and https://epicenter.works/content/eu-parliament-adopts-the-covid-pass-risks-for-data-protection-and-new-forms-of

4 See Article 4 paragraph 2 of Regulation (EU) 2021/953 and https://epicenter.works/content/five-reasons-to-claim-victory-on-the-eu-digital-covid-certificate

5 See https://identity.foundation/peer-did-method-spec/, https://identity.foundation/didcomm-messaging/spec/, https://openid.net/specs/openid-connect-self-issued-v2-1_0.html and https://w3c-ccg.github.io/ldp-bbs2020/

has to be verified (disability, age, etc.). Since the Wallet App aims to become ubiquitous and widely adopted in all parts of society, this will only amplify the negative impact the eIDAS proposal would have on privacy and data protection rights.

Suggested Solutions

Similar to the EU Digital Covid Certificate, the Regulation has to provide for safeguards for privacy by design in the Wallet App. Therefore, we suggest reframing Article 6a (7):

> *"The user shall be in full control of the European Digital Identity Wallet. The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet* ~~***which are not necessary for the provision of the wallet services***~~*, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services* ~~***which are not necessary for the provision of the wallet services, unless the user has expressly requested it***~~*. Personal data eidrelating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held."*

Additionally, the technological specification of the Wallet App in the legal text needs to ensure that principles of privacy by design are uphold. The Regulation has to guarantee the unobservability of user interactions on the Wallet App in order to protect users from surveillance on how they use the Wallet. These amendments are necessary because delegated acts based on Article 6a paragraph 11 give the Commission the power to define how the Wallet has to work in practice. Delegated acts should be limited to update specifications in light of new technological developments, but design principles that fundamentally define the privacy impact of the technology need to be already enshrined in the Regulation. It is necessary to eliminate the reference to information "necessary for the provision of the wallet services" altogether in order to make sure that a Digital Identity Wallet is implemented in such a way that it does not require such information to function. Existing (self-souvereign) eID schemes demonstrate that such an implementation is possible.

Biometrics and smartphone security

The security of the Wallet software is certified by audit companies that according to Article 6c are designated by the member states and only made public to the other countries, not the public. The concrete criteria that have to be met by the Wallet software are again only defined six months after the Regulation is established by the Commission via delegated act.

According to Recital 11, the Wallet App could also rely on biometrics to authenticate the users and the same Recital also allows for the storage of authentication information in the cloud. Recital 21 references provisions in the Digital Markets Act that oblige core platform providers such as Google or Apple to allow to be inter-operable with ancillary services such as identification and states that this provision would allow Wallet Apps to gain access to the secure enclave hardware elements which store biometric information like fingerprints and facial recognition patterns on modern smartphones. Depending on the technical implementation this could be extremely troublesome as it could undermine smartphone security and potentially lead to the exposure of biometric information on cloud storages or government controlled Apps. Because all technical details are left to be specified in delegated acts after the law has already been adopted, it is very hard to assess the privacy and

security implications of these broad powers given to the providers of Wallet Apps and the draft Regulation opens up high risks in this regard.

Similar to the unknown technical specifications of the Wallet App, the Regulation is additionally turning a blind eye to the vast differences in the security of smartphones. The Wallet App will naturally depend on the security of the smartphone on which it operates. Low-income users will less often own state-of-the-art devices and in many cases will not even receive security updates from their vendors anymore. Less tech-savvy users will not be as skilled in keeping the operating system of their devices up to date or configured correctly. We already see an increase in cyberattacks on smartphones and with the Wallet App these devices have just become more interesting targets for identity theft. The digital divide we know today will be exacerbated with the current eIDAS proposal, as we already see a price difference with analogue / in-person government services becoming more expensive than eGovernment services relying on eIDAS certified means of identification[6].

Suggested Solutions

The only solution to the security problems of the current framework is to further specify in the Regulation the technical requirements and architectural safeguards for privacy and security of the Wallet App and to have a broad discussion about it already now, instead of blindly trusting the Commission to do this work five months after the co-legislative process is concluded.

An inclusive solution for the different security levels of smartphones would be to include in the eIDAS Regulation an anti-discrimination obligation towards citizens or residents that decide not to use the Wallet App, may it be because they do not own a smartphone (with an adequate security level).

Breaking web security by forcing root certificates in every browser

According to Article 45 in the Commission's proposal, providers of web browsers would be obliged to include Root Certificate Authorities (CAs) from member states in their products. CAs underpin the security of encrypted https web traffic and authenticity of websites. Providers of web browsers have strict rules which CAs they include in this trusted list and are often facing pressure from governments to include country CAs for the purpose of spying on the web traffic of citizens. Setting a precedent here for the inclusion of state CAs could seriously undermine the security infrastructure of the web, enable more surveillance of encrypted web traffic and subsequently strengthen anti-democratic tendencies.[7]

Suggested Solution

Keep the original version of Article 45 of Regulation 910/2014 and drop the new wording in the new Regulation.

Mandatory identification before every attribute check

The current wording of Article 6a(4)(d) suggests that electronic attestation of attributes requires the previous authentication of the user by the relying party. This contradicts the essential privacy-preserving feature of selective disclosures by which, for example an age verification would not expose the real name of a person or their full birthdate. In Recital 29 such selective disclosures are a clear goal of the Regulation and have the benefit of not revealing additional information about the person.

6 https://www.wien.gv.at/english/e-government/transportation/parking/residents/parking-permit.html

7 See https://www.eff.org/deeplinks/2021/12/eus-digital-identity-framework-endangers-browser-security and https://blog.mozilla.org/netpolicy/files/2021/11/eIDAS-Position-paper-Mozilla-.pdf

Article 3(5) conflates the concept of authentication with identification – effectively allowing for the tracking of every individual that attests an attribute about themselves in the Wallet App in every online or offline use case.[8]

Suggested Solution

The attestation of attributes should not mandate the previous authentication or identification of the user to the relying party, also not with a pseudonymous identificator.

2nd order effects of cheap electronic identification

In the past years we have seen several attempts at the national and European levels to establish a real name obligation or mandatory identification for users of social media or video sharing platforms.[9] These attempts have often failed because the simple cost of officially identifying a user online makes it impractical to apply on a wide scale. This will change if the Wallet App lowers the price of identification of users on the internet in Europe to practically zero.

As obtaining verified identity information from users is enriching the personal data already collected, many actors will be incentivised to acquire this information from users. Current practice shows that users are easily tricked into consenting to give away their information and many of them do not have the necessary interest or understanding. One potential consequence would be the combination of targeted advertisements with verified identities. ..

Driving forces supporting this proposal

The Covid-19 pandemic was a catalyst for the eIDAS reform. In lockdown the practical need for eGovernment services and eCommerce became obvious to a majority. Additionally there are certain interdependencies with the NIS2 directive that required the Commission to reform the 2014 eIDAS Regulation. In total this proposal seems rushed by the Commission. The economic interests behind the proposal include for instance Trust Service Providers, who want to extend their business cases with this Regulation and make themselves more important. The Wallet App for natural persons has to be offered free of charge, but for legal persons there can be a fee for offering the software.

A widely used eID system creates many subsequent parts of industry that would like to participate in such a system. The banking sector is a prominent one that wants to reduce the cost of complying with know-your-customer (KYC) requirements. In the financial sector there are other actors that would like to focus the targeting of their financial profiling (liquidity scores, fraud detection, etc.). In several EU countries mobile providers have similar KYC requirements that could benefit from such technologies. In some countries media companies would like to offer advertisements based on very high quality targeting taking advantage of eID data. Lastly, the eCommerce sector would want to implement this technology to save costs and increase compliance in the long run.

8 See chapter 2.3 https://brusselsprivacyhub.eu/publications/the-european-commission-proposal-amending-the-eidas-regulation

9 See https://www.politico.eu/article/austrian-conservatives-want-to-end-online-anonymity-and-journalists-are-worried/ , https://netzpolitik.org/2021/tkg-novelle-seehofer-will-personalausweis-pflicht-fuer-e-mail-und-messenger-einfuehren/ and https://netzpolitik.org/2021/digitale-dienste-gesetz-eu-koennte-anonyme-uploads-auf-pornoseiten-verbieten/