Analysis of 5th eIDAS compromise from Czech Council Presidency

Analysis of 5th eIDAS compromise from Czech Council Presidency

This analysis was conducted by the digital rights NGO epicenter.works on 21. October 2022. For contact, please reach out to team@epicenter.works. Find a list of abbreviations below.

Summary

The trend of the Czech Presidency that first became apparent with the third compromise text continues. Industry interests are ranked above fundamental rights concerns of citizens. We see a further eroding of safeguards previously introduced by the Commission and French Presidency. This will make trialog more difficult, as we observe the opposite trend in the ongoing negotiations of the lead ITRE committee where data protection safeguards have been strengthened in the last compromise texts by the rapporteur. With the adoption of the LIBE opinion – given their exclusive competency on data protection issues – this positive trend in the Parliament is evident. Yet, the trajectory of the text under Czech Presidency will make finding a compromise on key issues from a citizen's perspective increasingly difficult.

Regulation of Use Cases

The EUID Wallet is a powerful tool as it offers a general purpose technology for identification, authentication and attribute verification of natural and legal persons vis-à-vis public authorities and private companies, online and offline. However, there are many very likely scenarios of abuse, fraud and identity theft in this new system which will hold, among other things, government issued identity information, sensitive health data and inlcude the function to legally sign contracts. Hence, it was applauded by the data protection community that the French Presidency, since the first compromise version, obliged relying parties to register their own use cases with their respective Member State of establishment according to Article 6b. Critically, this safeguard was enforced in Article 6a(5)(e) by the limitation within the EUID Wallet to only allow the relying party to ask information from a user that is in accordance with the approved registration by the Member State. This idea of the Council was picked up by almost all committees in Parliament. Thanks to this safeguard a hotel check-in can't ask intrusively for family composition or financial data, a liquor seller or bouncer has to check the 18+ requirement via selective disclosure, instead of asking for full name and birthdate, and employers or Russian border guards can't demand a copy of all the credentials in a user's EUID Wallet.

The Czech Presidency has completely removed this critical safeguard in Article 6b bit by bit. In the current text, the question whether there even is a registration of relying parties is left to every Member

State and potential sectoral legislation. This means the baseline for the new eID system shifts in the direction of a wild west regime where checks of relying parties are optional and one-sided notifications, reduced to the name of the relying party, are the rule. Critically, the Parliament has taken the opposite approach. The report of the rapporteur gives Member States the right in Article 6b(2) to revoke the registration of a relying party in case of illegal or fraudulent use of the EUID Wallet. Nevertheless, the switch from registration to one-sided notification of relying parties also means that the given name of the relying party might not necessarily be checked (by every Member State). In light of the fact that the users share government certified information about themselves, this seems unbalanced. Given the 80% penetration goal of the European Commission by the end of this decade, we can assume a user base of several hundred million citizens. This is an attack surface lucrative enough for elaborated cyber attacks. Safeguards to prevent fraud and expel abusing actors shouldn't be optional features that *might* come later – particularly, as the success of the eIDAS reform very much depends on the trust among citizens, which is earned hard and lost easy.

The Czech Presidency introduced the concept of "[hybrid] offline use" and "fully offline use" of the EUID Wallet in its third compromise version with an aim to lower the requirements for relying parties to register with a Member State. In the current fifth compromise version only "offline mode" remained. As noted in our previous analysis, this "offline" operation mode is, as definded by the EUID Wallet, not required to access remote systems. This definition is deeply flawed as the relevant processing of personal information is happening on the side of the relying party and it can happen irrespectively of whether or not there was a server connection at the time the information was obtained from the user. Such a special operation mode with lower regulatory requirements would make sense if the definition would limit the functionalities of the Wallet in such scenarios to only 1) zero-knowledge attribute attestations, 2) revocable pseudonym authentications or 3) selective disclosures of attributes that, even in conjunction, can't be qualified as personal data under Article 4(1) of the GDPR. Hence, a lower entry barrier for relying parties that limit their use of the EUID Wallet to functions without data protection impact would be welcomed! This would help proliferate the EUID Wallet, while achieving a strong incentive for relying parties to follow data minimalism and privacy-by-design principles. Examples are age verifications in physical commerce situations where the barrier to entry for shop owners and SMEs should be as low as possible and the registration of relying parties might not be necessary. But the current proposal simply creates a regulatory loophole to an already watered-down system of safeguards.

Unobservability and Privacy by Design

A central question for the success of the Wallet is whether or not users are in control about who sees their data. The Commission's proposal acknowledged this problem by requiring the data about how citizens are using the Wallet in their daily lifes to be kept logically and physically separated from all other data held by the issuer. The Parliament has taken a more privacy-friendly position by requiring that the architecture of the eID system shall be such that such data about user behaviour never exists in the first place, thereby fulfilling the GDPR requirement of privacy by design. This assurance level of unobservability is following the example of the EU Digital COVID Certificate Regulation (EU) 2021/953. Under the Czech Presidency we have witnessed the opposite development. The requirement of physical separation of this sensitive data has ben scraped and no further effort to prevent a panoptical

view of user behaviour has been undertaken. Trust in the system highly depends on the level of privacy assurances users can rely on. A centralised system with full observability might be deemed acceptable for rare eGovernment interactions that take place only several times a year. But an EUID Wallet with use cases such as online authentication at VLOPs, public transport tickets, hotel room keys, fitness club memberships, health and financial information that can't give the highest assurances of unobservability will be seen by large parts of the population as a panoptic nightmare.

The adopted LIBE version of the text and the one currently negotiated in ITRE extend the unobservability-principle even to issuers of the electronic attestation of attributes as to prevent them from obtaining knowledge of how their attributes are being used. An example that is prevented by this safeguard is a university keeping track of all the places where a graduate shows their diploma. Similarly, the requirement of zero-knowledge attestations as the default can be found in adopted provisions in LIBE. ITRE, too, is currently addressing this as a technological requirement for relying parties to make sure they are not able to obtain information other than the user has explicitly consented to share.

The Czech Presidency has undertaken improvements in Recital 29 on the definition of selective disclosures. Similarly, we welcome the clarification in the definition of "authentication" in Article 3.

Unique Identification

The Czech Presidency makes attempts to mitigate the fundamental rights concerns that arise from the obligation to uniquely and persistently identify all citizens of the European Union. Such an obligation raises serious constiutional concerns in Germany and would run counter to existing administrative practices in the Netherlands and Austria. The identifiers could be abused to track and profile users across interactions or relying parties. The use of these identifiers was originally limited to legal KYC scenarios and the first compromise text from the Czech Presidency attempted to even extend the scope to vague and undefined "administrative practices". Since the fourth compromise version this dangerous extension of scope has been removed and now the scope is again limited to legal KYC scenarios. Most importantly, the Czech Presidency is providing an alternative to unique and persistent identification in the form of record matching, while at least one such unique and persistent identifier is mandatory according to Article 11a of the Compromise. Recital 17a entertains the option of sector specific identifiers – which can cause a privacy disaster in jurisdictions with social media KYC, as this identifier would allow for the correlation of user behaviour across most online services – or relying party specific identifiers (also called "pairwise pseudonimity") – which would be the preferred option. It would be desirable to limit all KYC scenarios, where such an identifier needs to be transmitted, to relying-party-specific identifiers, whereby tracking of the user across relying parties would effectively be prevented.

Article 11a(2a) and Recital 17a create an obligation for Member States to provide organisational and technical measures to ensure high data protection and prevent the risk of profiling. The last obligation is impossible for Member States to fulfil in the current framework, as unique and persistent identifiers inherently enable the relying party to track and correlate user behaviour across interactions and potentially also globally across relying parties. There is no technical safeguard against this

mathematical certainty. A solution would be to fine-tune the scenarios in which certain identifiers are used, for example to solely rely on pairwise pseudonimity and record matching for the private sector.

Left unclear is the implication of the obligation to include a unique and persistent identifier in the minimum data set of PID in Article 12(4)(d). Article 6a should include clear provisions concerning the exposure of this identifier in non-KYC scenarios not governed by Article 11a. Following the principle of privacy by design, no unique and persistent identifiers should be exchanged with relying parties outside of legal KYC scenarios and as a fallback such identifiers should be derived from the PID as to be different for different relying parties (pairwise pseudonimity), thereby *at least* preventing the tracking of users across relying parties.

Non Discrimination

Since the announcement of the eIDAS reform in June 2021 a promise has been made that the use of the EUID Wallet has to be voluntary for citizens. But no steps were undertaken to ensure that this promise to citizens is actually upheld. All four committees of the European Parliament have adopted or are currently discussing non-discrimination provisions to protect those that will not use the EUID Wallet. Senior citizens, homeless people and people that don't have a smartphone or lack the digital literacy to operate the EUID Wallet safely would otherwise be marginalized.

Access to services, particularly government services, justice, the labour market and freedom to conduct business shall not be restricted or hindered for persons not using the European Digital Identity Wallet. Where essential services are provided and access to those requires the use of the European Digital Identity Wallet, easily accessible alternatives should be offered by the service provider. Additionally, several Parliamentary committees have enshrined in Article 45a the guarantee for acceptance of paper based attestations of attributes.

Web Security concerns arising from QWACs

The security concerns that arise from the mandatory inclusion of certificates from TSPs in web browsers as QWACs are referenced, but not solved. This problem is only mentioned in the non-binding Recital 32, which in the fifth version of the compromise text even limits the remedies available to web browsers to address potential security breaches at TSPs to only individual certificates. This means legal uncertainty for web browsers in the scenario of a security breach at a TSP, which would seriously undermine the possibility of web browsers to keep their users secure. Additionally, the problem of TSP certificates being misused for traffic interception by public authorities remains unaddressed. Given the fact that the rapporteur decided to delete Article 45 altogether in her report to ITRE, it seems unwise for the Council to ignore the security concerns raised by experts and not to offer remedies for the justified grievances.

Next Steps

The fifth compromise text was circulated on 19. October 2022 by the Czech Presidency. It will be discussed on 25. October 2022 and potentially at the 27. October 2022 Council Meetings. The aim is

to agree on a General Approach on 6. December 2022 and to enter into trialog negotiations under Swedish Council Presidency in 2023. The ITRE committee is scheduled to vote in November 2022 and to adopt a first reading position in the European Parliament in December 2022 / January 2023. The EUID Wallet can be expected to be live as early as 2024.

Abbreviations

eID… electronic Identity
KYC… Know Your Customer
PID… Person Identification Data, as defined in Article 12(4)(d)
TSP… Trust Service Provider
QWACs… Qualified Website Authentication Certificates
EUID Wallet… European Digital Identity Wallet
GDPR… General Data Protection Regulation, meaning Regulation (EU) 2016/679
VLOPs...Very Large Online Platforms, as defined in Article 25(1) of the DSA Regulation