DIGITALEUROPE

28 MARCH 2023

Towards more effective and coherent electronic identification in Europe

Executive summary

Europe's single market will greatly benefit from a stronger framework for electronic identification and trust services, and DIGITALEUROPE supports the ongoing efforts for a reform of the eIDAS Regulation.[1]

As trilogues between the European Parliament and the Council begin, some changes are necessary for an effective revision. The final text should:

- Be coherent with the existing framework and models, to ensure present investment is further developed rather than set aside;
- Prolong issuance and implementation timeframes to 24 months to allow adequate time for testing and development through large-scale projects;
- Allow for different methods to implement a high level of security as opposed to imposing logical and functional separation;
- Ensure that the European Digital Identity (EUDI) Wallet can function with existing unique identifiers across the EU, and set clear roles and responsibilities to the parties responsible for sorting EU citizens' records;
- Introduce safeguards to allow web browsers to react to security breaches and take precautionary measures in recognising qualified web authentication certificates (QWACs);
- Align the electronic identification language with existing legislation, such as the Interoperability Framework and the Payment Services Directive;[2] and
- Allow for the collection of information and combination of personal data for identity fraud prevention and detection purposes, in compliance with EU data protection law.

[1] COM/2021/281 final

[2] Commission Implementing Regulation (EU) 2015/1501 and Directive (EU) 2015/2366, respectively.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Aligning existing infrastructure and EUDI Wallets

The evaluation study of the eIDAS Regulation revealed several shortcomings, which included the lack of accessibility to online services by EU citizens, residents and businesses.[3]

To resolve those shortcomings, the proposal introduced a EUDI Wallet, without replacing nor annulling the existing eIDAS framework. However, the proposal does not offer a clear rationale for how the EUDI Wallet will help solve problems with the current eIDAS Regulation, how it will be better enforced, or how the new technology can add value to the existing infrastructure and investments.

By contrast, the proposal offers a much lower level of recognition of electronic identity schemes and signatures that have been notified and evaluated by Member States under the current eIDAS Regulation, and that use eIDAS nodes. It therefore sets aside past investments instead of developing them.

By setting an obligation to exclusively accept the EUDI Wallet, the proposal reduces the proven value of existing electronic identity schemes, which could result in unfair competition. The new framework should instead allow the use of existing infrastructure and enable a smooth transition.

We support the objective of ensuring a common approach and technical architecture for EUDI Wallets, and believe that international standards ISO/IEC 18013-5 (mobile driving licence) and 23220 (mobile eID systems) should be building blocks for the EUDI Framework and Toolbox.

Allowing for the testing and adoption of these standards would provide significant benefits, including reaching a high level of security by ensuring that the EUDI Framework meets sufficient levels of assurance to authenticate identities, enabling proof of a real identity and of a citizen's ownership thereof. Alignment with international standards would also be welcomed in the context of fraud prevention.

Implementation timeframes

The proposal envisages that Member States must provide the EUDI Wallet within 24 months of the implementing acts coming into effect. It also imposes that both the public and private sectors adopt the EUDI Wallet in their services. For private sector entities, this would be no later than 12 months after it has been made available by Member States.

The proposed 24-month timeframe is unrealistic, since the proposal and its implementing acts will set significant requirements for the EUDI Wallet, and present-day solutions do not yet meet the new requirements.

[3] SMART 2019/0046.

EUDI Wallet-like products still have to be developed from the ground up. To this day, there are only very few standards or comprehensive technical descriptions that would correspond to the proposal. For instance, the Architecture and Reference Framework does not amount to a final set of specifications, and is set to be updated following the final agreement on the proposal.[4] Additionally, if no definite certification scheme is released by the time the new Regulation enters into force, there would be no market security evaluation schemes for the EUDI Wallet.

We are concerned that time and procedural pressure could result in immature products being pushed to the market without adequate time for testing and development through large-scale projects. This would hurt security and healthy competition for vital EU infrastructure.

The obligation on service providers to accept the EUDI Wallet within 12 months creates great pressure in terms of both investment and compliance. DIGITALEUROPE recommends that the issuance and implementation timeframes be prolonged to 24 months. Alternatively, the proposal should loosen the requirements on the EUDI Wallet to encourage market-based competition and innovation.

Furthermore, Art. 45 should clarify that the requirements for QWACs and their recognition by web browsers shall only be imposed after the application deadline set by the related implementing act.[5]

Qualified attribute attestation services

Logical and functional separation

DIGITALEUROPE welcomes the proposal's ambitions to reinforce security through attribute attestation services. However, the final text should focus on defining the intended outcome, rather than imposing specific technical measures with the requirement of a logical and functional separation for qualified attribute attestation service providers.

Logical separation entails that qualified trust service providers, or any other service providers that already have an evaluated and highly secure infrastructure in place, should set up new and separate infrastructure. This would result in increasing upfront investment, which may deter potential service providers. Increased costs will negatively impact the availability of services on a wider scale, e.g. in cross-border EU services, and potentially their security. For this reason, the new framework should allow for different methods to implement a high level of security as opposed to imposing logical and functional separation.

[4] ARF v1.0.0.

[5] The same applies to other implementing acts, such as under Arts 45c and 45d.

The revised Regulation and its implementing acts must ensure that service requirements do not become overly restrictive for qualified trust service providers. The text should set out the outcome to be achieved with security measures, whilst leaving more granular security measures to implementing acts and technical standards.

Lastly, the newly introduced electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source represents an important development. It will be vital to ensure the same oversight standard for public sector bodies acting as issuers of electronic attestation of attributes as it does for trust service providers, either as issuers of electronic attestation of attributes or qualified electronic attestation of attributes.

Unique and persistent identifiers

DIGITALEUROPE welcomes the proposal's aim to facilitate unique identification, which could become a key success factor for an interoperable system across the single market. However, operating systems that are already in place in several EU countries should be recognised, so that the EUDI Wallet can function with existing unique identifiers in the EU.

However, the proposal's use of 'unique and persistent identification' appears incomplete. Art. 3(55) of the proposal implies that identifiers may not be considered unique until they are matched in another information system. Such match may subsequently be changed by the user. The identifier could therefore evolve and would not actually be *persistent* over time.

Furthermore, the proposed method of 'record matching' in Art. 3(55) does not determine the party responsible for sorting the records of the EU citizen of the Member State where they are residing at the time records were created, nor of the Member State where the records are actually kept.

Setting clear roles and responsibilities for parties to manage and provide data would address these problems and enable natural persons to collect their historical records, e.g. diplomas, social security records, property ownership or business registry records, from different sources in different Member States.

Qualified website authentication certificates

Art. 45 of the proposal obliges web browsers to recognise QWACs that meet certain minimal criteria. This obligation could result in negative implications for the security and privacy of European citizens and businesses.

Browsers would have to admit certificate authorities issuing QWACs without any control of misuse, such as domain impersonation or phishing. More broadly, the efficiency of QWACs in preventing cybersecurity threats and incidents has not been sufficiently demonstrated, whilst best practices for website authentication have been developed by the digital industry for years, including for the display of information on web browser interfaces (UIs).

Art. 45 should at least introduce safeguards to allow web browsers to react to security breaches and take precautionary measures, and to ensure that UI layout implications are reasonable and proportionate.

Electronic identification

To ensure legal certainty and predictability, DIGITALEUROPE recommends clarifying the mention of 'strong user authentication' in Art. 12(b)(2). One solution would be to align the wording with existing legislation, such as the Interoperability Framework and the Payment Services Directive.

Under the Interoperability Framework, specific reference is made to 'national ID documents' and 'unique identifiers constructed by a Member State,' covered by either national law or contractual obligations. Art. 3 of the eIDAS Regulation and Section 1 of Annex 1 of the Interoperability Framework pursuant to Art. 12(8) of eIDAS Regulation, define the terms 'authentication,' 'electronic identification' and 'person identification data.' Such language should be replicated in Art. 12(b)(3) to exclude simple account registrations and logins, instead of imposing separate obligations on VLOPs, which are a group of private relying parties.

DIGITALEUROPE also recommends better alignment with the PSD2 language, notably 'strong customer authentication,' which should be recognised within Art. 12(b)(2).[6] In Arts 3(50) and 12(b)(2) and Recital 31, any reference to 'strong customer authentication' should apply to verifying the identity of a user (natural or legal person).

Lastly, the scope of the EUDI Wallet acceptance obligations in Art. 12b(2) ought to be more clearly defined, so that it pertains to 'remote online services using distance communication.' This is to ensure that acceptance obligations are not extended to physical means of payment and authentication, such as card-based transactions, which would require disproportionate investment from the financial services sector.

Fraud prevention

The proposal does not allow the issuer of the EUDI Wallet to collect information about the use of the EUDI Wallet, nor to combine personal identification data and any other personal data in or related to the use of the EUDI Wallet with personal data from any other services offered by the issuer or a third party.

Whilst it is understandable that the restriction's purpose is to provide control to end-users over the use of the EUDI Wallet and their data, we believe that such provisions must not impede the prevention, monitoring and detection of identity

[6] Directive (EU) 2015/2366.

fraud, all of which play a crucial role in the secure issuance and usage of the EUDI Wallet.

Ensuring fraud prevention is essential, because the introduction of the EUDI Wallet is expected to make provisioning and usage of online services easier, more secure and consistent, and to enhance end-users' trust in the EUDI Wallet and online services. DIGITALEUROPE recommends the final eIDAS should spell out that the collection of information and combination of personal data for identity fraud prevention and detection purposes, in compliance with EU data protection law, is permitted.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Beatrice Ericson

Officer for Privacy and Security Policy

beatrice.ericson@digitaleurope.org / +32 490 44 35 66

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world's best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 102 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Applied Materials, Amazon, AMD, Apple, Arçelik, Arm, Assent, Autodesk, Avery Dennison, Banco Santander, Bayer, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, CaixaBank, Cisco, CyberArk, Danfoss, Dassault Systèmes, DATEV, Dell, Eaton, Epson, Ericsson, ESET, EY, Fujitsu, GlaxoSmithKline, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, Honeywell, HP Inc., Huawei, ING, Intel, Johnson & Johnson, Johnson Controls International, Konica Minolta, Kry, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Meta, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe, NEC, Nemetschek, NetApp, Nintendo, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Pearson, Philips, Pioneer, Qualcomm, Red Hat, RELX, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Skillsoft, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Czech Republic: AAVIT
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: Infobalt
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: Adigital, AMETIC
Sweden: TechSverige, Teknikföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT Ukraine
United Kingdom: techUK