bitkom

Position Paper

Bitkom on the eIDAS 2.0 Council´s General Approach

Background and Initial Statement

Rebekka Weiß, LL.M.
Head of Trust & Security

T +49 30 27576 161
r.weiss@bitkom.org

Clemens Schleupner
Policy Officer Digital Identity & Trust Services

T +49 30 27576-424
c.schleupner@bitkom.org

Albrechtstraße 10
10117 Berlin

The European Council published its General Approach for the EU Commission´s proposal for a regulation establishing a framework for a European Digital Identity on 25 November 2022. The EU Commissions proposal aims to review the eIDAS Regulation from 2014 in order to extend its benefits to the private sector and promote trusted digital identities to all European citizens and legal entities. Bitkom strongly supports the proposal's objectives, introducing a streamlined European legal framework for secure public electronic identification and trust services, facilitating and giving people access to public, private and cross-border digital transactions. However, the proposal lacks both linguistic clarity and technical specifications concerning the implications of several suggestions entailed in the proposal. Since the proposal touches upon a wide range of industries, including Banking, Travel, Education, etc., simplified and unclear language that leaves room for interpretation and thus insecurities can be detrimental for concerned industries and, as a consequence, the success of the EU Digital Identity.

The EP should also consider that rolling out the EUID Wallet completely and streamlining separate and individual national eID solutions will take a considerable amount of time. Public and private sector alike need more time and clear guidelines to provide the national frame- and groundwork eIDAS 2.0 requires from the EU Member States. Against this background we support the extension of the implementation deadline of the Council's General approach.

Summary

Bitkom welcomes the aim of the proposed regulation to introduce a European Digital Identity Wallet and to ensure universal access for people and businesses to secure and trustworthy electronic identification and authentication. It also welcomes the goal of streamlining the European eID ecosystem and to promote cross-border digital operations. However, some key suggestions have the potential to put a disproportionate level of responsibility on relying parties and would work against an easier and more secure way for digital identification. Furthermore, the language leaves too much room for interpretation and is thus causing a high level of uncertainty. Nevertheless, Bitkom supports the introduction of a EUDI Wallet.

General Requirements

Level of Assurance

Currently, the draft Regulation takes a broad approach to the services within its scope and does not fully consider the technical and legal constraints that apply to different services and industries.

The legislative proposal sets the assurance level for the newly introduced EUID Wallet "high" as a benchmark. This has far-reaching implications both for the consumer and for concerned businesses. Currently, a number of national eID solutions are based on a "substantial" security level. In order to include those eIDs in existence, that would currently not uphold the envisaged standard of the EUID Wallet, the Council suggests an additional remote on-boarding procedure "that together meet the requirements of LoA high". Such an on-boarding procedure is to be rejected if the remote identity proofing procedure is not based on the ETSI TS 119 461 standard and/or the new CEN TC/224 WG20 standard for PID onboarding.

Similarly, the proposed assurance level "high" for the issuance of a qualified certificate or qualified electronic attestation of attributes does not reflect the existing market requirements. Experience with certificates for almost a decade give proof that a substantial level of assurance is sufficient for qualified certificates. To meet the requirements for a high level of assurance, any qualified trust service provider will have to take extraordinary measures to "ensure the identification of the person with a high level of confidence". Upgrading the required level of assurance would exclude the majority of currently used verification methods and pose serious threats to the existing market of trust services established by eIDAS. It is crucial to keep the LoA "substantial" to issue and use qualified certificates at least until the EUID Wallet becomes a serious, secure, and widespread identification method. Otherwise, any new or current identification procedures, e.g. video-ident, would become insufficient once this regulation comes into effect, which would mean an immediate end to the qualified trust services as we know it.

Furthermore, we argue against the setting of “minimum technical specifications, standards or procedures with respect to the verification of identity”. Setting only a minimum standard will cause a more fragmented ecosystem as Member States will then define their own requirements on a national level. This will not only drive the attempt to harmonize the European ecosystem obsolete, but also cause a market disadvantage for service providers in stronger regulated Member States. We call upon the EP to provide a clear definition of the future standard for the Member States to implement.
Bitkom however supports the issuance of an EUID Wallet based on an LoA “high” in the future.

Retention period

Bitkom suggests defining a specific time limit up to which information concerning data issued and received by the qualified trust service provider shall be recorded and kept accessible.

Creating relevance

The success of EUID wallets is measured by their actual, regular usage, which is fuelled by the number of use cases and an attractive user experience. The mandatory linking of the usability of the wallet to a valid identity issued by the member state, which requires citizens to physically verify their identity before using the wallet, creates a higher onboarding-barrier than necessary. Therefore, the regulation should provide the possibility to use the wallet separately from the national ID, if the user wishes to do so. The step of proofing one’s identity according to the criteria of eIDAS 2.0 and link the ID to the wallet can be carried out as soon as it is required by a specific use case, providing the user with the possibility of “upgrading” their wallet. Nevertheless, the wallet can already be used for applications prior to that. Consequently, a broader range of daily use cases in both the private and public sector would be created, including those, where proof of identity is not required. This would also clarify the wallet’s principal role as a tool for authentication that can be used for identification in connection with identity linked to the wallet.

Moreover, public and private sector ID solutions should complement each other. This requires the use of different wallets in a compatible and interoperable form, not only between member states, but also between different national providers.

Relying parties

Currently, the draft regulation takes a broad approach to the services within its scope and does not fully take into account the technical and legal constraints that apply to different services and relying parties in the Member States.

An unconditional acceptance obligation of the EUDI Wallet for those private relying parties currently included under the proposal is inappropriate when aiming for an efficient and user-friendly digital ID ecosystem. From a financial services perspective for example, and with a view to payment services, a general application of the acceptance obligation to physical means of payment and authentication media such as the established card-based transactions will cause disproportionate implementation efforts whilst not adding immediate value to the customer journey. In order to achieve the needed legal clarity in this horizontal regulation in line with its intention, we propose the use of already existing, legally defined terminology. It is advisable to clarify that the obligation for the acceptance of an EUDI Wallet pertains to remote online services using distance communication.

While Bitkom supports the obligation for relying parties to notify their respective Member States of their intend to rely upon EUID Wallets in their services, we advocate for an automated way of determining the list of relying parties, for example by parsing machine readable lists that are published by the Member States. We furthermore reject the possibility for Member States to exempt relying parties from the notification requirement. In order to guarantee transparency and data protection the consumer needs to be fully aware as to who is accessing their EUID Wallet.

QWACs

As we have stated in a previous positioning, Bitkom regards the obligation of web-browsers to recognize Qualified Certificates for Website Authentication (QWAC's) as an important element for strengthening European Digital Sovereignty, the European Digital Market as well as consumer protection. We also strongly support the Council's amendment which expands the obligation to adopt implementing acts for specifications and reference numbers of standards to paragraph 2 of Art. 45.

QEAA

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. We would nevertheless like to stress that the proposal should apply the same oversight standard for the issuers of QEAA and EAA as it does for QTSPs. Furthermore, the regulation shall define the standards necessary for the verification of attributes against authentic sources, similar to single digital gateways.

Archiving and Preservation

The Regulation does not sufficiently differ between "archiving" and "preservation" of electronic data, such as electronic signatures, electronic seals, etc. We strongly suggest

clarifying the definition of these two concepts to showcase their respective delineation.

Notification of breaches

Under the current revision, identifiable affected individuals and other relevant competent bodies are to be notified of any breaches or disruptions in the provision of services defined in the regulation, within 24 hours after the incident. For practical reasons this timeframe should be extended to 72 hours, leaning on the data security framework of the GDPR.

Audits

Regular audits of qualified trust service providers are an important quality management tool. We are thus in favour for regular audits taking place at least every 24 months. However, we would like to point out that informing the supervisory body about planned audits and allow for the participation as an observer will create an unnecessary bureaucratic boundary and could potentially lead to overstraining the supervisory body.

Security and consumer protection

Bitkom welcomes the proposal's attempt to strengthen digital authentication procedures in order to provide a more secure user-experience and to promote cross-border digital transactions. We would like to encourage the EP to review the possibility of cloud-based solutions for data storage of the EUID Wallet. A centralized system bears a number of risks that should be avoided. We thus propose to focus on decentral solutions that gives the user full control over their stored data.

Conclusion

We support the aim to revise the eIDAS Regulation by introducing measures to streamline fragmented European legal frameworks for secure public electronic identification and to grant EU-citizens and legal entities access to secure digital identities. However, for eIDAS 2.0 to be as effective as possible, a number of clarifications, especially on the technical side, have to be made. The revised proposal also must consider the different levels of advancement of EU Member States concerning LoAs as well as the overall use of digital identities. We are determined to proactively improve and develop the legal framework and eager to discuss our abovementioned concerns to find solutions.

Bitkom represents more than 2,000 companies of the digital economy. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.