Position Paper

of the German Insurance Association (GDV)

ID-number 6437280268-55

on the

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

Gesamtverband der Deutschen Versicherungswirtschaft e. V.

German Insurance Association

Wilhelmstraße 43 / 43 G, 10117 Berlin
Postfach 08 02 64, 10002 Berlin
Phone: +49 30 2020-5000
Fax: +49 30 2020-6000

Rue du Champs de Mars 23
B - 1050 Brussels
Tel.: +32 2 28247-30
Fax: +49 30 2020-6140
ID-Nummer 6437280268-55

Contact:
BDIT;
European Office

E-Mail: **bdit@gdv.de; bruessel@gdv.de**

www.gdv.de

Contents

1. Introduction
2. Distribution
3. Anti-money laundering & taxes
4. Technical implementation
5. Data Protection
6. Conclusion

Executive summary

The German insurance industry welcomes the developments at the European level and the introduction of a European identity scheme (EUid) in combination with the proposed amendments of the Regulation (EU) No 910/2014 (eIDAS) by the European Commission. The proposed approach to establish an EU-wide ecosystem on digital identities in form of a European identity scheme (EUid) is to be supported.

Digital and secure identification of natural and legal entities gains in importance in an increasingly connected world. It is the basis for digital processes in administration and business. At the same time, digital identification must be both secure and user- and business-friendly.

The introduction of a European identity scheme (EUid) might facilitate identification process for customers and businesses provided that the technical and administrative requirements will be proportionate.

1. Introduction

Digital identities represent a core component in a connected world – no matter if it concerns the public or private environment. This involves unambiguous digital communication between business-to-customer (B2C), business-to-business (B2B), government-to-citizen (G2C) and the Internet of Things (IoT). It is essential that these are based on secure and trustworthy technology, while at the same time enable the identity owner to use it in a user-friendly way.

The increasing digitalization of processes in insurance companies requires the facilitation of digital identity verification. Insurance Companies and end users are often dependent on complex, partly analog processes, especially in initial identification and subsequent authentications. Hence, a need for leaner processes in digital identity verification, technical facilitation in the know-your-customer (KYC) principle, and an improvement in user-friendliness is given. The introduction of a Europe-wide uniform digital identity (EUid) could be an approach to this.

2. Distribution

Concerning distribution, the industry welcomes the initiative and recognizes a lot of potential in the insurance environment. In the area of distribution, the following use cases might be possible, for example

- Clear and easy identification of potential customers, in particular regarding online distribution channels.
- Simplifications within the application process, no need to check and copy id-cards - „digital friendly environment “, in particular in the compliance with requirements under money laundering law (see chapter 3)
- Ensuring that applicants are of legal age and therefore have full legal capacity. For underage applicants, easier and more secure identification of both parents or other legal guardians.

- Registration and access to the insurers' online services - Identification for single sign-on or TGIC
- ability to prove that the requirements for initial qualification as well as continuing training and development (according to Art. 10 IDD) have been fulfilled.
- Potential use cases:
  - Clear identification of examination participants of the expert knowledge examination and for participants of continuing trainings
  - Proof of continuing training and development to the supervisory authorities, e.g., by linking a "well-advised" account with the wallet and transmitting the information to the NCA.

3. Anti-money laundering and taxes

The introduction of an EUid as an additional method offers potential with regard to KYC processes for the prevention of money laundering and terrorist financing. The need for appropriate remote and practical identification methods became particularly apparent during the Corona pandemic. AML/CTF obliged entities should be able to use the EUid for AML-compliant remote identification. The design of an EUid should therefore be consistent with (current and upcoming) AML requirements. Although an EUid could offer added value in the future, it is crucial that the already established identification procedures can continue to be used as long as an EUid has not yet found the necessary customer acceptance and dissemination. Therefore, the procedures already established for AML-KYC purposes (especially videoident procedures) for remote identification must not be called into question and, in addition, the flexibility for new, innovative procedures must be maintained.

Once the procedure has been successfully established, the EUid could also be used for tax identification and thus represent a voluntary supplement to the existing national tax identification numbers.

4. Technical implementation

Article 6a of the proposed amendment introduces digital wallets based on self-sovereign identity (SSI) technology. Member States are therefore required to provide wallet solutions to their natural and legal persons 12 months after enforcement of the amendments. According to Art. 6a (4) No. c, the European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance ‘high’.

SSI is based on blockchain architecture. Data is stored in a decentralized and tamper-proof manner. The SSI-blockchain-infrastructure is thus a decentralized blockchain network with IT security and trust mechanisms. The end user determines which data is transmitted during an identity check and thus owns full data sovereignty. This enables the involved stakeholders to verify the authenticity, origin, and integrity of the digital proofs without the SSI blockchain knowing the owners or the proofs issued. The implementation of SSI or SSI-like solutions requires a certain degree of standardization and interoperability, similar to transmission and network protocols on the Internet (e.g., TCP/IP protocols). However, such a uniform IT-architecture, or a test catalog for SSI-architecture does currently not exist but is required for the establishment of an ecosystem.

At the national level various initiatives were established for developing digital wallet-solutions based on SSI-technology on different levels of assurance – mainly on the level of assurance “substantial”. A mutual and equivalent recognition of identities will be of crucial importance for

a smooth functioning of the ecosystem. This has to be considered when defining technical and legal frameworks.

In addition, wallet solutions based on SSI run only on very few devices currently on the market. This has to be considered to avoid a limited access to the ecosystem for a small number of citizens. Thus, the EUid system should be technically open to other already existing wallets, which are available on a higher number of devices regardless their operating systems.

5. Data Protection

When deciding on a specific technology for the implementation of digital identity wallets, care must also be taken to ensure conformity with data protection legislation (e.g., the principle of data protection by design) and to choose future-proof solutions. A solution that does not take this into account may become subject to regulatory friction, which could slow down the uptake of trustworthy digital identities and prevent a quick rollout of much needed digital identity wallets.

Berlin, 16. August 2021