spearIT
InfoSec · Compliance

eIDAS 2.0 & SSI

A Preliminary Analysis of Opportunities and Risks

table of contents

Disclaimer: This document is a preliminary, point-in time analysis of the (draft at the time of writing) eIDAS 2.0 Regulation, scoped specifically to the articles related to the concept of self-sovereign identity.

foreword

On June 6th, 2021, the European Commission announced the launch of a European Digital Identity together with an improvement proposal to the current eIDAS regulation in response to the announcement made by the President of the European Commission the previous year. Among others, the upcoming eIDAS version foresees new types of trust services based on self-sovereign identity (SSI).

In the new proposal, not only will all Member States be *obliged* to provide certified digital wallets to citizens, but businesses will also have to accept them as forms of identification, opening-up the applications of government-issued digital identities to the private sector.

SpearIT, having active involvement and participation in eIDAS working groups and providing expertise knowledge at the national level, has performed a preliminary analysis on those eIDAS 2.0 provisions which are related to the SSI technology and identified the potential opportunities and risks introduced by these new provisions.

basic terminology

eIDAS: stands for "electronic IDentification, Authentication and trust Services" and refers to a regulation in the European Union that sets standards for electronic identification and trust services for electronic transactions in the internal market.

eIDAS 2.0: In June 2021, the European Commission proposed an update to its pan-European digital identity framework. It will enable every European to have a set of digital identity credentials that are recognized across the EU – otherwise known as European Digital Identity (EUDI) Wallets. These 'wallets' are mobile applications or cloud services that collect and store digital credentials and allow them to be used secretly and securely for numerous government and non-government use cases.

SSI: Self-sovereign identity (SSI) is a term used to describe the digital movement that recognizes an individual should own and control their identity without the intervening administrative authorities. SSI allows people to interact in the digital world with the same freedom and capacity for trust as they do in the offline world. This is called "self-sovereign" identity because each person is now in control of their own identity. The SSI identity system gives users the freedom to selectively disclose and authenticate the particular attribute(s) related to their overall identity using cryptographic mechanisms of digital wallets, without disclosing the full information that comprises their identity, to dozens of databases each time you want to access new goods and services, with the risk of identity theft or privacy violations.

Verifiable Credential: a set of one or more tamper-evident claims/credentials made by an issuer which can be cryptographically verified.

Digital Wallet: it is a functional element/service that provides secure storage of verifiable credentials and private keys related to cryptographic operations on the contained credentials.

eIDAS 2.0 highlights

- Electronic identity (eID) services under eIDAS 2.0 will be available to any EU resident and business.
- EU Digital Identity Wallet Trust Mark, a clear, simple, and recognizable visual indicator that attests the compliance of a digital wallet service according to the
- eIDAS 2.0 will be compliant with the General Data Protection Regulation (GDPR).
- eIDAS 2.0 will move the control of identity and personal information to the end-user.
- Emphasis on the principle of sole control: this allows all EU citizens to exercise their rights to a digital identity that remains solely under their control (self-sovereignty).
- eIDAS 2.0 will improve the enablement of services in the private sector to cover every industry type.
- eIDAS 2.0 will facilitate the digital transformation of all sectors.
- New products and services will be offered based on self-sovereign identity, cryptography and blockchain, delivering a high degree of authenticity while also protecting customer privacy.
- The wallet will allow users to create and use Qualified Electronic Signatures (QES), which are accepted across the EU.

Article 3, point 16

New trust services with legal effect foreseen.

'trust service' means an electronic service normally provided against payment which consists of:

(a) the creation, verification, and validation of [...] electronic attestation of attributes and certificates related to those services; [...]

(f) the recording of electronic data into an electronic ledger.'

OPPORTUNITIES

The addition of these services in the trust services family, establishes the regulatory framework and pervades trust for using SSI products such as verifiable credentials stored in digital wallets operating on top of DLTs or blockchain networks, enabling legal effect in courts.

This offers a legal framework to the European Blockchain Services Infrastructure (EBSI) to establish itself as the blockchain provider for public services.

RISKS

The risk identified here is the scenario where an entity sets up a private blockchain network and registers data on it. In this case, even though the data may not have legal validity, they cannot be denied legal effect. This allows issuance of non-qualified verifiable credentials by an organization with malicious intensions to demand legal effect of the verifiable credentials in courts.

Another potential risk could be the closed provision of verifiable credentials, compatible only with a digital wallet provided by the issuer of the verifiable credentials, since the Regulation does not state directly that a verifiable credentials provider shall make them compatible with the EUID.

That could impede the standardization of the EUID Wallet as the sole, user-controlled digital wallet and drive the user to manage and operate multiple digital wallets, potentially with reduced/different levels of control.

Article 6a

EU Member States shall provide a digital wallet to citizens.

requires *Member States to issue a European Digital Identity Wallet under a notified eID scheme to common technical standards following compulsory compliance assessment and voluntary certification within the European cybersecurity certification framework, as established by the Cybersecurity Act [...]*

European Digital Identity Wallets ***shall*** *be issued:*

(a) by a Member State;

(b) under a mandate from a Member State;

(c) independently but recognised by a Member State.

OPPORTUNITIES

Of all the options, option (c) will possibly open the market of wallet providers to any type of high-quality providers and rule out the those who fail to provide adequate security or quality levels of service.

It is logically derived that competition will increase among digital wallet service providers.

RISKS

Option (a) poses a potential risk in case European governments build, offer, and promote their own digital wallet, which will lead to:

- cutting down market expectations
- minimizing or eliminating digital wallet **interoperability*** feature among Member States

Option (b) also poses a risk since it is possible that a Member State will release a public tender for a digital wallet service, which will likely lead allow large organizations or consortiums with plentiful of resources and experience in such procedures to win, excluding smaller, niche-market organizations with high expertise in this subject.

Option (c) seems the most neutral choice but any SSI provider, irrespectively of its size, shall comply with the Regulation and gain the EU Digital Identity Wallet Trust Mark, as it is currently happening in eIDAS compliant services.

Interoperability, **one of the 10 guiding principles of Self-Sovereign Identity, states that identities should be as widely usable as possible, allowing identification to cross international borders without users losing control of what information is shared. Users will be able to carry and maintain a portable digital identity across platforms and geographical locations, independently of the digital wallet service provider and/or verifiable credential issuer.**

For more information on SSI principles, have a look at Christopher Allen's Life with Alacrity blog.

Article 6a, point 3

Mandatory dual storage capability of qualified and non-qualified credentials for digital wallets.

"European Digital Identity Wallets shall enable the user to:

(a) securely request and obtain, store, select, combine and share, in a manner that is transparent to and traceable by the user, the necessary legal person identification data and electronic attestation of attributes to authenticate online and offline in order to use online public and private services;

(b) sign by means of qualified electronic signatures.

OPPORTUNITIES

The addition of qualified electronic signatures in the digital wallet enables the offering of value-added services and the usefulness of wallets in daily activities. This simplifies the life of citizens that cannot currently take full advantage of an electronic signature for various legal reasons in their place of residence.

It is obvious that the EUID Wallet may become a single, powerful data vault which could manage also digital money.

RISKS

Adding complexity to a product or service usually introduces delays and deviations to the initial development and release roadmap. That may be a potential outcome in the EUID Wallet, having a wide family of trust services included.

Article 12b

EU Digital Identity Wallet acceptable in the private sector and obligatory in cases where strong user authentication is required.

Where private relying parties providing services are required by national or Union law, to use strong user authentication for online identification, or where strong user authentication is required by contractual obligation, including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a.

Where very large online platforms as defined in Regulation [reference DSA Regulation] Article 25.1. require users to authenticate to access online services, they shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a strictly upon voluntary request of the user and in respect of the minimum attributes necessary for the specific online service for which authentication is requested, such as proof of age."

OPPORTUNITIES

The mandatory nature of the EU Digital Identity Wallet establishes the ground for a market; thus, making the digital wallet and verified credentials a market enabler and a success factor of itself.

Articles 12c & 14

Member States can accept credentials issued by other Member States without peer agreements.

Article 12c - Mutual recognition of other electronic identification means:

"Where electronic identification […] is required under national law or by administrative practice to access an online service provided by a public sector body in a Member State, the electronic identification means, issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that online service, provided that the following conditions are met […]"

Article 14 – International aspects:

"[…] trust services provided by providers established in the third country concerned shall be considered equivalent to qualified trust services provided by qualified trust service providers established in the Union.'

OPPORTUNITIES

Initially under eIDAS, mutual recognition of notified eID schemes between Member States required a bilateral process which proved lengthy and sometimes complex and thus, an obstacle in the wider cross-border use cases adoption.

eIDAS 2.0 will offer easier interoperability since only two elements are adequate for cross-border identity attributes recognition, given that the necessary assurance levels for electronic identification are achieved:

1. a certified digital wallet
2. qualified trust services for electronic attestations

This will be true also for non-EU digital wallet providers since the Regulation allows the opportunity for such providers to offer services to the European market.

RISKS

The widening of the market with the above provisions leads to more competition, since non-EU providers who may have greater experience on the topic of SSI, digital wallets and verifiable credentials could offer competitive solutions in comparison to EU-based providers who might entered the market very recently.

eIDAS Compliance & Consulting Services

SpearIT, being actively involved in the evolution of the eIDAS ecosystem through participation in EU Commission's working groups, cooperative studies among Member-States, conformity assessments, consulting and engineering, provides a full-fledged solution to support and provide guidance to service providers to achieve compliance with the requirements of eIDAS 2.0 Regulation and the applicable technical standards foreseen.

Our current service portfolio includes eIDAS compliance projects delivered in the following sectors:

- Advanced & Qualified eSignatures & eSeals
- eTimestamps
- Qualified Web Authentication Certificates (QWACs)
- Electronic Identification (eID) Schemes
- Electronic Registered Delivery services (eRDS)
- Preservation Services (PresS)
- Validation Services (ValS)
- Identity Proofing Services (IdPS) / Remote User Onboarding

SERVICE PROVISIONS

- Gap analysis of the current state of your candidate products/services and of your organization
- Consulting on gap elimination
- Consulting on documentation and legal matters
- Consulting on actual technical implementation
- Planning & execution of the conformity assessment
- Periodic maintenance of your compliance status through advisories and ad-hoc consulting

Talk to an eIDAS expert at **www.spearit.net**

SPEARIT

Egnatia 154 st,

Thessaloniki, 54636

GREECE

p: +30 2311 320 262

w: spearit.net

e: info@spearit.net