Report on the European Digital Identity Framework and eIDAS Regulation Amendment

1. Introduction

When I began looking into the European Digital Identity Framework, I discovered that the EU is working to unify digital identity across all Member States. This effort builds on the original eIDAS Regulation (EU No 910/2014), which set standards for electronic identification and trust services. But now, with this amendment, the EU aims to make digital identity simpler, more secure, and accessible across borders. They're focusing on creating a Digital Identity Wallet that everyone in Europe, including businesses, can use for everyday needs.

It seems the EU institutions and Member States are working together closely on this wallet project. The idea is to give everyone the ability to control their identity information and use it easily when they need it. I get the sense the EU wants to make online interactions more seamless and safe. It's exciting, but there are also some concerns.

2. Overview of the European Digital Identity Framework

From what I understand, this framework aims to fix inconsistencies by standardizing digital identities across the EU. Previously, each country had its own system, and that led to a lot of fragmentation. The new approach is for everyone in the EU, whether they're citizens, residents, or businesses, to have access to one unified digital identity system.

The Digital Identity Wallet isn't a standalone tool but part of a larger system with electronic identification (eID) schemes and interoperability protocols. With this wallet, people should be able to safely store identity information and share only specific

details when needed. For example, users could verify their age without showing their entire ID, keeping more personal information private.

3. Structure and Functions of the EU Digital Identity Wallet

I found some unique features in the Digital Identity Wallet. One is the emphasis on user control, allowing users to share only the data they choose, when they choose. You could store details like your name, qualifications, or date of birth and only disclose what's necessary for specific purposes. This sounds like a solid privacy approach.

Another interesting feature is the use of FIDO (Fast Identity Online) technology, which would make the wallet password-free. FIDO relies on secure methods like biometrics or hardware tokens to authenticate users, removing the need for vulnerable passwords. I think this is a smart move to strengthen security, especially with so many risks tied to passwords.

Then there's the privacy aspect. The wallet incorporates techniques like zero-knowledge proofs (ZKPs) and possibly Z-SNARKs, which are cryptographic methods allowing verification without revealing actual data. For instance, you could verify that you're over 18 without showing your birth date. I think this approach respects privacy, but I wonder if people will fully understand what's happening behind the scenes. These cryptographic proofs are complex, and not everyone feels comfortable relying on "black-box" security, where they're protected by processes they don't fully see or understand.

4. Security Challenges with the EU Digital Identity Wallet

As I dug deeper, I found that the security setup with FIDO introduces some challenges. FIDO is designed to resist phishing by tying authentication to your device, but this raises issues when moving across devices. I think the EU will need to standardize how data transfers securely across multiple devices, which could be a challenge.

Device Attestation: A big part of FIDO's security depends on device attestation, which checks if a device is secure enough. However, if the wallet depends heavily on device attestation, there's a risk of intruding on user privacy. Some worry that attestation requirements might end up allowing a form of surveillance, where devices reveal more information than users realize. I'm not sure where the line should be drawn here, but it's something the EU needs to consider carefully.

Exclusive Access Requirements: FIDO's most secure methods rely on hardware, like Trusted Platform Modules (TPMs) or Secure Elements (SEs), which are only available on newer or high-end devices. If the EU mandates hardware-based security, it might unintentionally exclude people who can't afford the latest devices. It seems like a tough balance—strong security versus broad accessibility.

5. Cryptographic and Legal Concerns with Cross-Border Data Verification

The EU framework also aims to make sure the wallet works across borders, which is great in theory. However, using privacy-preserving tools like ZKPs in a cross-border system might be trickier than it sounds.

Legal Interoperability: Some countries might not fully recognize ZKP-based proofs generated in other Member States. This could mean someone's identity might be verified in one country but not accepted in another. I wonder if this lack of "legal interoperability" could slow down the EU's vision for full digital mobility. Aligning legal standards for ZKPs across so many countries could be complicated and time-consuming.

Regulatory Resistance: I've noticed that some regulators are hesitant to embrace ZKPs because they're hard to fully understand and audit. Privacy-preserving cryptography, while effective, can feel like a "black box" to regulators, and that lack of transparency could lead to resistance. I think the EU might face some hurdles in convincing all Member States that ZKPs are trustworthy and reliable for identity verification.

6. Offline Functionality and Security Risks

The EU’s framework also emphasizes that the wallet should work offline, but this adds another layer of security challenges.

Offline Authentication: In offline mode, it’s tough to maintain security without real-time verification. Without regular checks, there’s a risk that some attestations may expire or be tampered with. For instance, FIDO depends on real-time checks, so adjusting this for offline scenarios could weaken its effectiveness. I think the EU will need to find a way to balance offline access with security.

7. Ethics of Data Pseudonymization vs. Anonymization

The wallet will use pseudonyms or anonymous data in many cases to protect users, but this raises questions about just how anonymous users will be.

Limitations : Although it is effective, it can sometimes be reversed or re-identified. For instance, if pseudonymized data is combined with other available information, there’s a risk that the user’s identity could be revealed. This makes me wonder if pseudonymization truly offers enough protection. Some experts think anonymity should be the goal, but achieving true anonymity is complicated and can limit how effectively the wallet can verify identities.

I think the EU should explore more advanced anonymization techniques if they want to maximize user privacy, but this might mean sacrificing some functionality in the wallet’s verification process. It’s a tricky balance, and I’m not sure if there’s a perfect solution.

8. Conclusion and Future Prospects

When I think about where this is heading, I see the Digital Identity Wallet simplifying access to public and private services for EU residents and businesses alike, making it quicker and more secure. However, the journey to full adoption faces complex challenges, particularly in security and privacy, especially with FIDO authentication.

The EU will need to keep updating its technology and standards to address emerging security threats.

Looking at the larger picture, there are significant hurdles with interoperability. Member States will need to harmonize national electronic identification schemes to avoid inconsistencies. This unified approach is essential if the wallet is to work seamlessly across borders, yet achieving this kind of standardization is difficult when each country has distinct legal requirements and security standards. I think that, without a shared legal and technical foundation, this framework might struggle to function consistently.

Privacy protection is another crucial factor, and while the wallet promotes user-controlled data sharing, there are concerns about how personal data will be handled by third parties. The wallet's use of selective disclosure techniques, like zero-knowledge proofs (ZKPs), is promising, but I wonder if people will fully trust these complex cryptographic methods. Some users may find it hard to understand how ZKPs work, making transparency and education critical.

Then there's the issue of data sovereignty and storage. The document suggests that data might be stored locally or in the cloud, but this raises questions about cybersecurity and data access across Member States. A cloud-based solution might make data access easier, but it could also expose users to cybersecurity risks if not protected by state-of-the-art encryption.

In the future, I think we'll see more sophisticated privacy tools and secure storage solutions integrated into the wallet to make it even safer. The EU has set high standards, but there's always room for improvement, especially as new security concerns arise. Regular vulnerability assessments, as outlined in the regulation, will be key to ensuring ongoing security.

Overall, while I see a lot of potential in this framework, careful monitoring, technical adjustments, and legal harmonization will be crucial to keep everything running smoothly and build user trust across the EU.