Developers Alliance's feedback to the European Commission's Inception Impact Assessment on the Revision of the eIDAS Regulation – European Digital Identity (EUid)

The Developers Alliance welcomes the opportunity to provide feedback on the European Commission's planned revision of the eIDAS Regulation.

[Developers Alliance](#) advocates on behalf of software developers and the companies invested in their success, to support the industry's continued growth and promote innovation.

1.   We support the importance of trusted digital identities in the private sector. Trusted identities are a key enabler of the digital economy where developers are active, and where interactions often occur between parties without established relationships. The ability to build systems that replace physical seals and signatures with digital equivalents is fundamental to bringing legal relationships online.

2.   We also support the use of trusted digital identities in the public sector. Relationships between governments and citizens often encompass highly confidential or personal issues (taxation, benefits, healthcare, etc.) and trusted digital identities are a key enabler of security and privacy in these contexts.

3.   The market for trusted digital identities is already well established. Through existing relationships with governments, financial institutions, communications providers, and online ecosystem providers, EU citizens have a robust foundation for secure digital economy services. Any proposed revisions to existing law must take care not to disrupt what's working naturally.

4.   As the Internet of things grows in importance, the extension of trusted digital identities to encompass agents, sensors and actuators will increase. Trusted identities will likely play a role in future cybersecurity and authentication systems for AI and IoT. Any proposed revisions must take into account the dynamic and evolving nature of the digital economy and the infrastructure it rides on.

5.   The current limitations of eIDAS systems, including their fragmented nature and lack of consistency and ubiquity, have limited their utility. Since the launch of the eIDAS Regulation, market forces in the private sector have evolved to provide many of the benefits envisioned by the previous rules. These private sector trusted digital identity ecosystems have become widely used and provide very sophisticated protection for digital economy participants. They continue to evolve and improve driven by market competition.

6.   We believe that the private sector is fully capable of developing sophisticated digital identity services, benefiting from the continuous innovation that a competitive marketplace promotes. We do not believe that a single, public sector replacement is either required, or desirable. Where a common or compatible system with universal application is beneficial, we are confident that the market will coalesce on this solution (as has happened in credit card payment and other systems in the past).

7.   We agree that the status quo is no longer valuable, having been overtaken by private sector innovation and implementation. Re-investing in this scheme is unlikely to drive consumers away from private sector alternatives. As such, we are not generally in favor of Option 1 under the proposed Revision alternatives.

8.   While we support the potential benefit of extending eIDAS support to the private sector digital identity market (Option 2), we remain wary of regulations which could restrict the tremendous innovation taking place. Any intervention in this area must avoid diluting the commercial potential that attaches to these services - otherwise investment will stop and consumers will be harmed. Defining in advance the restrictions that would attach to this Option has the potential to make it unpalatable to potential private sector partners. A better

regulatory solution would be to engage the private sector BEFORE placing pre-conditions on the hypothetical solution (a basic tenet of good regulatory practice).

9.   Respecting consumer preference, including choice in authentication is a key consideration for online businesses. The control of personal data is already guaranteed by the GDPR, and any relevant additional rules should be carefully assessed against it. We agree that certain authentication options which are disconnected from a verified physical identity makes fraud (such as identity theft) and cybersecurity threats more difficult to mitigate. Private service providers, including online platforms, could integrate with the public eID systems in order to confirm their users' legal identity.

10.   Extending the eIDAS service to directly compete with existing private sector alternatives (Option 3) is likely to fail. While a common framework for public and private sector services would be extremely valuable, displacing a thriving and increasingly sophisticated and effective market with a bureaucratic system is unlikely to yield a better product.