



Response to the European Commission's Roadmap on European Digital Identity

INTRODUCTION

On behalf of the Center for Data Innovation (datainnovation.org), we are pleased to submit feedback to the European Commission's roadmap titled "Inception Impact Assessment for Revision of the eIDAS Regulation – European Digital Identity (EUid)."¹ In this submission, we summarize the three policy proposals under consideration and provide feedback on each option.

The Center for Data Innovation is the leading think tank studying the intersection of data, technology, and public policy. With staff in Washington, D.C. and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as open data, cloud computing, and the Internet of Things. The Center is a non-profit, non-partisan research institute affiliated with the Information Technology and Innovation Foundation (ITIF).

BACKGROUND

In 2014, the EU adopted the eIDAS (electronic identification, authentication, and trust services) regulation to establish a cross-border framework for electronic IDs (eIDs) and "electronic trust services" (e.g. electronic signatures, time stamps, electronic seals, etc.) in EU member states. Unfortunately, only 15 out of 27 member states offer cross-border eIDs, the national rules on digital identity remain fragmented across member states, and few member states offer eIDs that can be used for commercial purposes, such as online banking or online shopping.

The Commission is seeking feedback on three policy options to address the current shortcomings, including by modernizing the regulatory framework for digital identity and establishing a new eID for EU citizens (EUid).

¹ European Commission, "Inception Impact Assessment for the Revision of the eIDAS Regulation – European Digital Identity (EUid)," <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-European-Digital-Identity-EUid->



Option 1: Revise eIDAS

Option 1 would revise the eIDAS regulation to improve consistency and interoperability across member states. This option could require member states to provide citizens with eIDs by a certain date, establish security standards for solutions, and create guidelines on cost, liability, and interoperability for the private sector.

Option 2: Extend eIDAS to the Private Sector

Option 2 would propose legislation to extend the scope of the eIDAS regulation to the private sector and introduce new electronic trust services, such as for identifying devices. This option would consider establishing specific data protection requirements for digital ID service providers, such as restricting providers from reusing data collected for identification purposes without the explicit consent of users.

Option 3: Introduce a European Digital Identity (EUID)

Option 3 would introduce a European Digital Identity scheme (EUID) to complement the existing eIDAS regulation. Citizens could use the EUID to access public and private online services, and its use would be voluntary. This option may include a requirement that online service providers recognize the EUID.

FEEDBACK ON PROPOSED OPTIONS

The European Commission is correct that the status quo is failing to provide all citizens access to an eID accepted across the EU and the lack of a secure, interoperable eID solution limits digital commerce. To address these shortcomings, the Commission should pursue elements of each policy option discussed above. Specifically, it should develop more guidelines for eIDs offered by member states to ensure quality, security, and interoperability. It should also revise the eIDAS regulation to allow the private sector to use government-issued eIDs and introduce electronic trust services for identifying devices. Finally, to provide a fallback option for any member states that fail to offer eIDs, the Commission should establish an EUID available to any EU citizen. However, the Commission should be careful not to overregulate private sector identity service providers who provide important electronic trust services and can provide consumer-facing tools to help users leverage the value of a government-issued eID. There is no need to set additional data protection rules for identity services providers since they must already comply with the General Data Protection Regulation (GDPR). In addition, the eIDAS framework and the EUID should complement existing private-sector digital identity solutions by allowing private sector services to integrate with any government-issued eIDs.



Moreover, the Commission should not seek to exclude non-European service providers from offering identity services to EU citizens.

Option 1 would expand access to eIDs from member states. Indeed, any resident of a member state should have the right to quickly obtain an eID and this eID should be compatible across the EU. Option 1 would also harmonize security standards and features for eIDs across the EU. The risk is that the EU may not choose standards that facilitate interoperability with existing private sector solutions. To address this concern, private sector stakeholders, including existing identity providers, should have a role in developing standards.²

Option 2 would extend the scope of eIDAS to the private sector, thereby allowing private sector companies to use eIDs to authenticate individuals to commercial services. This is a welcome direction, as it would likely increase the use of eIDs across the EU and enhance security and privacy for individuals. This option would also expand the eIDAS regulation to create new “trust services,” such as identifying and authenticating devices. These types of identity services will be important with the growth of the Internet of Things, and the Commission should establish an interoperable framework for digital identities of electronic devices.

However, the Commission should not revise or expand data protection regulations for identity service providers. These service providers are already subject to the GDPR, and creating additional regulations would likely only discourage potential services providers from entering the market. In particular, the Commission should not discourage identity providers from sharing personal information about users with their consent. Many Internet users have accounts with social media platforms that they can use to authenticate their identity to other online services, such as to shop online. In many cases, consumers will want to share data from their digital identity providers for their own convenience and security.

Option 3 would establish a common eID that any EU citizen could use voluntarily. Given that many EU member states do not provide an interoperable national eID, providing an EUid would be a major asset to growing the EU digital economy. However, the European Commission should not use the development of an EUid to exclude foreign private sector identity service providers from the EU market or require the private sector to accept the EUid if they prefer to use an alternative. Instead, an EUid should complement private sector solutions that allow individuals to authenticate securely to online services. Many consumers use authentication services from companies like Google, Amazon, Microsoft, and Facebook, which allows them to securely manage their personal information and use convenient features like single sign-on. In addition, some startups have created “personal data

² Alan McQuinn and Daniel Castro, "A Policymaker's Guide to Blockchain" (ITIF, April 30, 2019, <https://itif.org/publications/2019/04/30/policymakers-guide-blockchain>).



wallets” to give consumers a variety of tools to manage their data and digital identity and choose how to share their personal data with others.

Unfortunately, the roadmap appears to oppose continued use of these types of commercial services, many of which consumers can access for free. The roadmap says, “Solutions of major social platforms offer convenience, which comes at the cost of losing control over disclosed personal data.” On the contrary, some social media platforms have made major investments in giving users granular control over their information and how they share it with others. If the Commission’s goal is to expand use of trusted identity solutions, it should work in partnership with the providers which many EU citizens already use and which third-party services have already integrated with. For example, private sector identity service providers could integrate with a government-issued eID to allow individuals to verify details of their legal identity.

The current eIDAS regulations are insufficient and the Commission is right to pursue substantial reforms to address the shortcomings. Providing individuals a legal identity is an inherent responsibility of government, and this responsibility should extend to the digital economy. The private sector can support these efforts, but it cannot solve this problem alone. Better standardization across EU member states would lead to greater adoption by the private sector. But the Commission should not seek to impose a public sector eID requirement that would limit EU citizens from using private sector digital identity solutions as this would reduce consumer choice and access to many secure, convenient, and easy-to-use services.