BETTER
IDENTITY
COALITION

Comments to the European Commission

eIDAS Inception Impact Assessment

September 2020

The Better Identity Coalition appreciates the opportunity to provide comments to the European Commission's (EC) on its recently published "Inception Impact Assessment" regarding the future of eIDAS.

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 22 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, fintech, payments, and security.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. While our primary focus is on the United States, our activities and ideas have started to gain international interest over the last year, and we have started to engage in venues abroad as well. More on the Coalition is available at https://www.betteridentity.org/.

In July of 2018, we published *Better Identity in America: A Blueprint for Policymakers*[1] – a document that outlined a comprehensive action plan for the U.S. government to take to improve the state of digital identity in the U.S.

At the core of our Blueprint is the idea that the private sector will not be able to solve digital identity challenges on its own. While the private sector continues to innovate in identity, government remains the only authoritative issuer of identity – and we are at a juncture where the government will need to step up and play a bigger role to help address critical vulnerabilities in our "digital identity fabric." Much of the Blueprint outlines an action plan for policymakers to establish new government digital identity services in a way that sets a high bar for security and privacy, with a focus on offering new choices for consumers.

Against that backdrop, we are encouraged to see the EC outline ways in its "Inception Impact Assessment" that the eIDAS initiative could be expanded to support greater private sector participation, as noted in the proposed Option 2 and Option 3. We offer several points for consideration on this matter:

1. **The limited scope of the eIDAS network today provides limited benefits; expanding eIDAS to the private sector would create positive network externalities that would create value for European countries, businesses, and people.**

   eIDAS today provides a valuable service to Europeans when they need to interact online with other governments in the European Union – but the number of cross-border consumer-to-government (C2G) use cases is small relative to the number of consumer-to-business (C2B) use cases. The fact that eIDAS does not support Europeans in cases where they need to prove their identity to private sector entities limits the relevance of eIDAS to many people,

[1] See https://www.betteridentity.org/s/Better_Identity_Coalition-Blueprint-July-2018.pdf

and precludes European people and businesses from realizing the full potential of cross-border digital identity infrastructure.

2. **The expansion of eIDAS to support private sector identity proofing needs could help industry solve a major challenge: how to reliably deliver high assurance, remote identity verification services for new account opening and account recovery.**

   Industry has produced some good tools to help companies with this challenge today, but given that government is the only authoritative issuer of identity, many of these private sector tools are trying to "guess" what only the government actually knows. The gap between what private sector tools can provide and what is actual "truth" in identity creates numerous inefficiencies and allows fraudsters and criminals to exploit remote identity verification processes for criminal gain.

   Governments can help to address shortcomings in the identity ecosystem by offering new services that modernize legacy paper-based identity systems around a privacy-protecting, consumer-centric digital model that allows consumers to ask the agency that issued a credential to stand behind it in the online world – by validating the information from that credential.

   An expansion of eIDAS to support identity proofing not only for government transactions but also those in the private sector would help private entities have a higher level of confidence with regard to who they are dealing with online and enable additional high-value transactions to be moved into the digital realm. As the Inception Impact Assessment notes: *"an extension of eIDAS to the private sector is likely to generate considerable economic gains through an increased offer and uptake of identification and authentication for activities intermediated online."*

3. **The United States has launched similar efforts – creating an excellent opportunity for cross-border collaboration.**

   While identity schemes vary from country to country, there are significant economic and security benefits to be realized through exploring ways to harmonize requirements, standards, and frameworks where feasible between countries. Focusing on international coordination and harmonization is one of five "pillars" of our Policy Blueprint.

   On that point: at a time when the EC is considering expansion of eIDAS beyond government applications, the U.S. government has also launched efforts to expand the reach of its various authoritative identity systems to support remote digital identity proofing requirements. In May 2019, the White House Office of Management and Budget (OMB) issued Policy M-19-17, ''Enabling Mission Delivery through Improved Identity, Credential, and Access Management."[2] The policy calls for:

> *Agencies that are authoritative sources for attributes (e.g., SSN) utilized in identity proofing events, as selected by OMB and permissible by law, shall establish privacy-enhanced data validation APIs for public and private sector identity proofing services to consume, providing a mechanism to improve the assurance of digital identity verification transactions based on consumer consent.*
>
> *These selected agencies, in coordination with OMB, shall establish standard processes and terms of use for public and private sector identity proofing services that want to consume the APIs.*

To date, one agency (the U.S. Social Security Administration) has launched a service aligned with this policy – the electronic Consent Based Social Security Number Verification (eCBSV) Service launched in July 2020.[3] Others are in the works in the months ahead. A similar set of services in Europe could offer new opportunities for international collaboration, including mutual recognition of identity schemes that could reduce trade barriers and enable more secure, frictionless cross-border commerce.

4. **Expansion could take the form both of allowing eIDAS to be used by the private sector for attribute validation to also encompass increased recognition of private sector identity providers.**

The future of the digital identity market is one of a "virtuous circle" where both the public and private sector each contribute elements that they are ideally suited to provide – and each make the other stronger.

- Government can help private identity providers create more high-assurance, robust credentials by validating identity information residing in government systems.
- Industry, in turn, can help government by 1) combining these validated attributes with private sector innovations to create more user-friendly high-assurance identity solutions, and 2) federating these high-assurance credentials with government services.

We do not have strong feelings as to whether something as ambitious as a new European Digital Identity scheme (EUid) as described in Option 3 is required to enable this vision of a "virtuous circle" to be realized. On one hand, it would help to provide a firm set of standards and operating rules to enable a broader digital identity ecosystem. Conversely, it may introduce layers of complexity that make it difficult or impossible to reach agreement

[2] See https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf
[3] More on eCBSV is at https://www.ssa.gov/dataexchange/eCBSV/

on critical issues. We have seen similar efforts struggle in other countries, given the complexity of the issues to address and variety of stakeholders to satisfy. Many of the benefits of an EUid ecosystem may be able to be obtained through more lightweight approaches.

5. **Consider mutual recognition and re-use of pre-approved eID products.**

   If a product has been approved for use with an eID scheme in one EU member state, it would be beneficial if the eIDAS initiative allowed for the same product to be approved for use in other eID programs as well. Such an approach could simplify the approval processes for eID schemes, as they could make use of common approved elements. This, in turn, could increase the rollout pace and adoption of eID schemes in the EU.

We greatly appreciate your willingness to consider our comments and suggestions, and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition's coordinator, Jeremy Grant, at jeremy.grant@venable.com.