Center for Democracy & Technology Comments to the EU-US Trade and Technology Council, Technology Standards Working Group, Subgroup on Digital Identity

March 2024

We welcome cross-governmental transatlantic coordination of technology standards for digital identity. Driven by a combination of legislative proposals, technical developments, governmental priorities, and industry opportunities, technology standards for digital identity are seeing intense activity. The multiple ongoing standards processes could benefit from coordination, engagement, direction, and support, particularly in promoting key public interest values.

We provide this brief comment primarily to highlight the important steps needed to protect and promote privacy, free expression, and other human rights in the development of standards and broader adoption of digital identity, particularly high-assurance government-issued digital credentials. The TTC has yet to focus on those issues in the mapping exercise, and it should not delay any further that necessary work. In order to be relevant and to provide support to the ongoing cross-sector, multistakeholder efforts to design effective digital identity standards, the TTC should contribute to identifying how protections for privacy and human rights will work across US and EC jurisdictions and what is needed in technology standards to enable those protections.

About CDT

The Center for Democracy & Technology (CDT) is the leading nonpartisan, nonprofit organization fighting to advance civil rights and civil liberties in the digital age. We shape technology policy, governance, and design with a focus on equity and democratic values. Established in 1994, CDT has been a trusted advocate for digital rights since the earliest days of the internet. In particular, CDT has long played a leadership role in technical standard-setting fora as a civil society voice.

I. Missing in the mapping exercise so far

The report emphasizes that "both sides of the Atlantic aim to provide easier and more secure access to online services to their citizens, with shared values of privacy, security, civil liberties, equity, accessibility, and interoperability."[1] However, the mapping exercise thus far has failed to compare how the frameworks address those values – particularly privacy, free expression, and freedom from discrimination and bias – and what is needed to protect them in cross-border interoperability of digital identities.

[1] US-EU Trade and Technology Council Working Group 1: Technology Standards, Subgroup on Digital Identity. (2023, December 22). *DRAFT EU-US TTC Digital Identity Mapping Exercise Report*. https://futurium.ec.europa.eu/system/files/2023-12/EU-US%20TTC%20WG1_Digital_Identity_Mapping_Report_Final%20Draft%20for%20Comment_22122023.pdf

We very briefly illustrate each of these issues, but are happy to collaborate on further explorations of each topic at a later date.

Regarding privacy, remote presentation of government-issued high-assurance identity credentials presents risks of widespread surveillance. There is a real danger of a “papers, please” Internet where users become accustomed to constant requests for their identity documents. Although this form of surveillance may sometimes be motivated by well-meaning aims to protect people, it may also be used to facilitate commercial interests in tracking and profiling or law enforcement surveillance unmoored from the rule of law.

Free expression and access to information are also implicated by threats to privacy. There is a chilling effect to speaking online or even seeking out information on controversial topics when that activity may be directly linked to one’s government-issued identity documents. Access to information may also be diminished by inappropriate restrictions on who may read or contribute to information on particular topics, like preventing teens from accessing information about reproductive health or LGBTQ+ advocacy.

Discrimination and bias should also be considered in any systematic review of digital identity. Easier access to digital identification over the Internet may facilitate inappropriate discrimination against people based on various personal characteristics, including age, race, country of origin, immigration status, or caste. There may be issues of bias in who is able to successfully obtain or present their credentials. Furthermore, many people may not wish to, or may not have the ability to, present digital credentials, particularly immigrants and people with less wealth or access to technology.

II. Gaps in the ecosystem

Lack of a consistent, comprehensible, and effective set of privacy protections is a large barrier to cross-border interoperability of digital identity technologies. If digital identity solutions are widely deployed in Europe and the United States without established and effective protections for privacy and other rights, the likely outcomes include:

- ubiquitous infringement of human rights;
- a lack of trust from the population in government and industry services, both within and between countries;
- legal challenges, especially to cross-border transfers or presentations of identities; and
- isolation and lack of interoperability.

The TTC does not yet appear to have a plan to take on the necessary work of collaborating on protections for civil liberties that can be applied to digital identity applications in the US, EU, and beyond. Although Section 4.2 of the report (“Next steps > Standards coordination and pre-standardisation research”) does identify some of the important questions that would benefit from

transatlantic (indeed, global) cooperative efforts, for the most part, these questions leave out how privacy, freedom of expression, and freedom from discrimination will be protected. For example, how will use cases for accessing government-issued credentials be regulated to prevent inappropriate requests? What is necessary for accountability for abuse of access to digital identities? How will governments ensure that use of digital credentials is truly voluntary? What technical, organizational, and legal protections will provide unlinkability (between different presentations, as well as between issuance and presentation) of digital identity credentials?

Technical standard-setting bodies, including ISO, W3C, IETF, and others, may not have the full breadth of expertise or representation to answer these types of fundamental policy questions, but as technical standards quickly progress, they need to address them. Without an understanding of how human rights will be protected, or how these systems will work for the needs of vulnerable populations (the first listed question), the technical designs and protocols that are developed will be inadequate at best, or actively harmful at worst. At a more basic level, developers of technical standards may not fully understand the legal protections (for privacy, free expression, and freedom from discrimination) – either in place or that have been proposed – in different jurisdictions, or how technology standards should accommodate them.[2] At W3C, we have been coordinating work on user considerations for digital credentials – including identifying risks to privacy and free expression, potential mitigations, and principles.[3] There have been extensive privacy reviews of existing credentials-related specifications, which may be one starting point for a broader review of the state of the art of privacy protections.[4] TTC could contribute to determining how rights can be protected across jurisdictions and what is needed in technical standards for those protections.

III. Critical use cases to consider

How residents interact with their governments, for example to access particular government benefits, may well be an appropriate and beneficial use of remote identification based on government credentials. Government agencies are particularly well-positioned to understand and develop this use case, including identifying the customers and requirements and existing legal and technical protections.

[2] The recently adopted eIDAS regulation, for example, includes some significant privacy safeguards, but will require significant implementation in technical standards to realize them. See:
Epicenter.works. (2024, 29 February). Potential & Risks of the European eID.
https://epicenter.works/en/content/potential-risks-of-the-european-eid

[3] Doty, Nick. (2024). *User considerations for credential presentation on the Web*. W3C Privacy Interest Group (PING).
https://github.com/w3cping/credential-considerations/blob/main/credentials-considerations.md

[4] For example, Verifiable Credentials Data Model v2.0 Privacy Considerations:
https://www.w3.org/TR/2024/CRD-vc-data-model-2.0-20240227/#privacy-considerations

We recommend that any cooperative effort on digital identity also directly identify and consider potential abuse cases: areas where digital identity technology is likely to be abused and where mitigations against abuse should be developed in advance.[5]

While not an exhaustive list, the following abuse cases may provide particular insight:

1. Online identity verification to track users' online browsing history for commercial surveillance,
2. Age verification to exclude young people from resources on sexuality and sexual health, and
3. Online discrimination against people by country of origin or immigration status.

IV. Future work

There is much work to be done to develop interoperable digital identity systems in such a way that they respect privacy and other human rights. Governments can play a significant role in advancing that work if they identify the values that they wish to uphold, detail what is needed to protect and uphold those values, and engage actively with multistakeholder communities. As the UN Human Rights Council recently noted, technical standards may either facilitate or inhibit the exercise of human rights, and states, such as the US and EU member states, have affirmative obligations to promote human rights in their participation in technical standard-setting; to formally evaluate the impact on human rights of new technical standards; to adopt legislation to foster respect for human rights; and to ensure the participation of a broad range of stakeholders in such standard-setting processes.[6] The TTC should take on the task of ensuring that its members fulfill these obligations.

[5] For an accessible overview of this technique in software security, see:
Hope, P., McGraw, G., & Anton, A. I. (2004). Misuse and abuse cases: Getting past the positive. *IEEE Security & Privacy*, 2(3), 90–92. https://ieeexplore.ieee.org/abstract/document/1306981/

[6] Office of the United Nations High Commissioner for Human Rights. (2023). *Human rights and technical standard-setting processes for new and emerging digital technologies*. United Nations Human Rights Council. https://digitallibrary.un.org/record/4031373