TTC WG1 DIGITAL IDENTITY SUBGROUP ROUNDTABLE WORKSHOP REPORT

THE TRADE & TECHNOLOGY DIALOGUE

Funded by the European Union

29 March 2023

AUTHORS: Camille Ford and Panka Rékasy

This report was written following the hybrid workshop of the Trade and Technology Council (TTC) Working Group 1 Digital Identity Subgroup held on 29 March 2023. This event was organised by the Trade and Technology Dialogue (TTD), which facilitated a half-day workshop on EU and U.S. digital identity initiatives.

The TTD is an EU-funded project, supporting the TTC by mobilising stakeholders and providing research outputs. It is a consortium of several organisations, based in the EU and the U.S. (CEPS, the EUI, IAI, Forum Europe and Providence Group).

Contents

Introduction

This event on digital identity brought together representatives from the European Commission, the National Institute of Standards and Technology (NIST), a Bureau of the U.S. Department of Commerce and EU-U.S. Trade and Technology Council (TTC) stakeholders to provide updates on the work of the Digital Identity Subgroup within TTC Working Group 1 (WG1): Technology Standards.

After opening remarks and stage-setting interventions by EU and U.S. government officials, technical experts from NIST and the European Commission presented advances in digital identity on each side of the Atlantic. From the U.S. government side, the presentation and discussion focused on NIST's digital identity programme and the recent fourth revision of NIST *Special Publication (SP) 800-63: Digital Identity Guidelines*. The European Commission presented European Digital Identity, including eIDAS 2.0 and current processes driving development of the EU Digital Identity Wallet (EUDIW). The technical presentations were followed by a panel discussion on the relevance of transatlantic cooperation for different use cases of digital identity.

Participants were able to engage directly with government representatives and subject matter experts throughout the workshop through hybrid Q&A sessions and an in-person post-event reception. A cross-section of TTC stakeholders from government, industry, academia and civil society attended both the high-level and technical presentations on digital identity.

Agenda

15:00 Opening remarks

Dr Laurie E. Locascio, Under Secretary of Commerce for Standards and Technology and Director of the National Institute of Standards and Technology (NIST), U.S. Department of Commerce

Dr Thomas Skordas, Deputy Director-General Communication Networks, Content and Technology, European Commission

15:10 Introduction & stage setting for the workshop

Co-Chairs of TTC Working Group 1: Technology Standards

Anthony Quinn, Team Lead, Office of Standards and Intellectual Property (OSIP), International Trade Administration (ITA), U.S. Department of Commerce

Thibaut Kleiner, Director, Policy Strategy and Outreach, DG CNECT, European Commission

15:20 Initial statements

TTC Working Group 1 Digital Identity Subgroup Co-Leads

Dimitrios Meritis, Senior Advisor for International Science, Technology, and Innovation Policy, National Institute of Standards and Technology (NIST), U.S. Department of Commerce

Vicente Andreu Navarro, Policy Officer, eGovernment and Trust, DG CNECT, European Commission

15:30–16:30 Presentations by EU and U.S. government representatives

Paolo De Rosa, Chief Technology Officer EUDIW, DG CNECT, European Commission

Ryan Galluzzo, Identity Program Lead, Applied Cybersecurity Division, National Institute of Standards and Technology (NIST), U.S. Department of Commerce

16:45–17:30 Panel discussion: The relevance of transatlantic cooperation for different use cases

Moderator: Andrea Renda, Senior Research Fellow and Head of the Global Governance, Regulation, Innovation and Digital Economy (GRID) Unit, Centre for European Policy Studies (CEPS) and Trade and Technology Dialogue Director

Panel

- **Connie LaSalle**, Senior Technology Policy Advisor, Applied Cybersecurity Division, National Institute of Standards and Technology (NIST), U.S. Department of Commerce
- **Gudrun Stock**, Deputy Head of Unit, eGovernment and Trust, DG CNECT, European Commission
- **Herbert Leitold**, Executive Director, Secure Information Technology Center – Austria
- **Carmine Auletta**, Chief Innovation and Strategy Officer at InfoCert and Member of the Board of the Cloud Signature Consortium
- **Hannah Quay-de la Vallee**, Senior Technologist, Center for Democracy & Technology (CDT)
- **Julianna Cafik**, Principal Standards Architect, Microsoft

Stakeholder Engagement by Numbers

Figure 1.

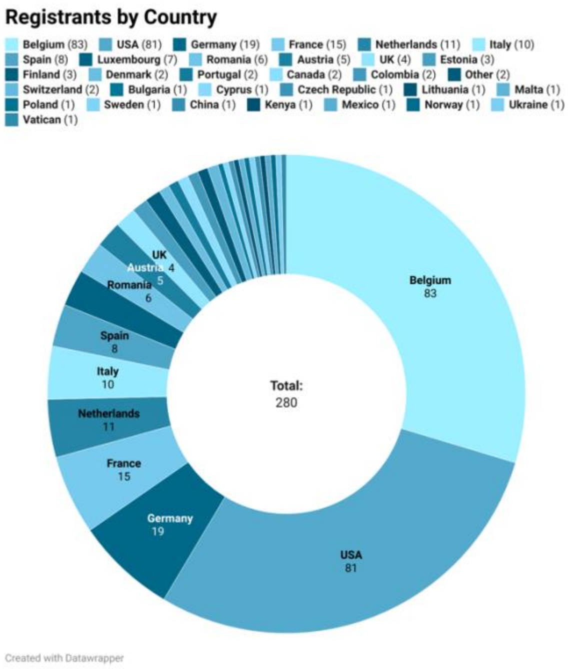


Figure 2.

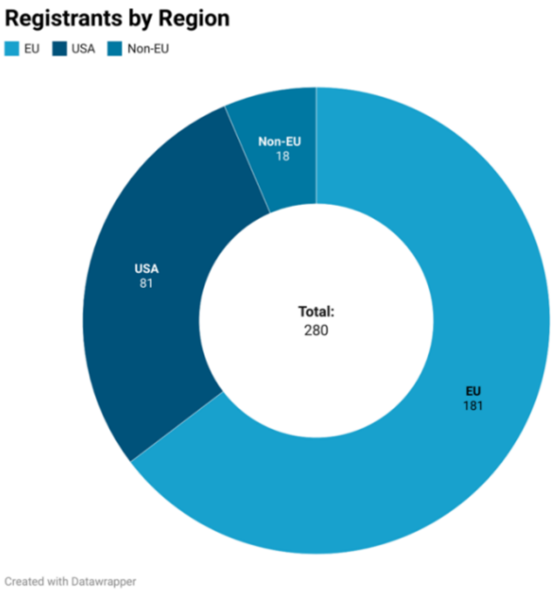
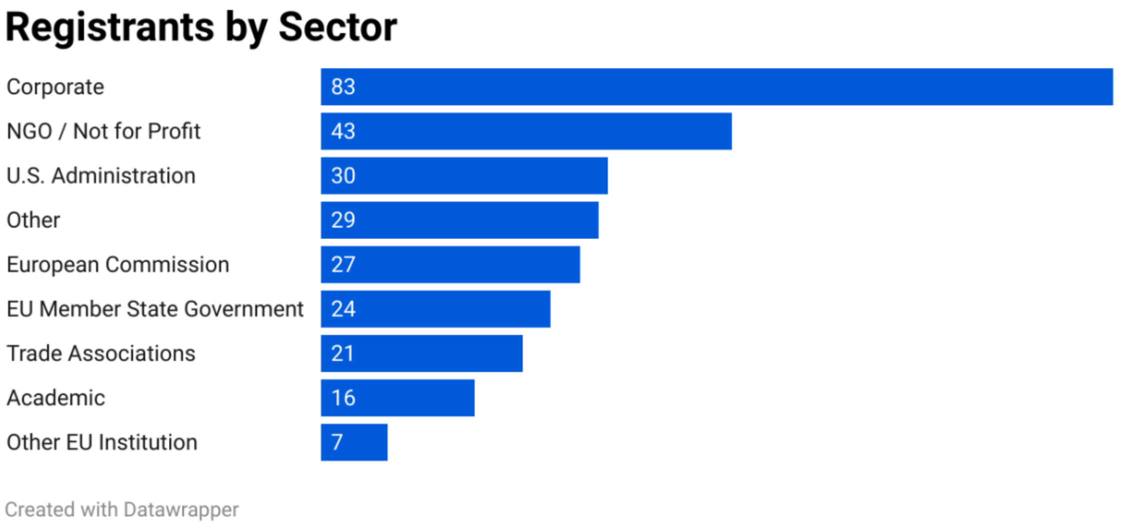


Figure 3.



Summary of the event

Opening remarks by **Dr Laurie E. Locascio**, Under Secretary of Commerce for Standards and Technology and Director of the National Institute of Standards and Technology (NIST)

Dr Laurie Locascio opened the workshop by highlighting the essential and challenging nature of the TTC's objectives. She emphasised the importance of growing transatlantic capacities in pre-standardisation research, and how this underpins U.S. and EU contributions to international standards development – a key priority for NIST.

Given the present backdrop of global competition, Dr Locascio also noted the pivotal role that the standards play in dictating the markets of tomorrow. Current international standards that are technically sound and that facilitate access to global markets have already benefited the public on both sides of the Atlantic – and will continue to do so. In this light, the EU and U.S. must continue to work closely to uphold and ensure the integrity of international standards and the organisations that generate them.

The WG1 Subgroup on Digital Identity is a clear illustration of the importance of this cooperation. As such, Dr Locascio previewed the presentations to come by noting the fourth revision of the NIST *Special Publication (SP) 800-63: Digital Identity Guidelines*. It seeks to respond to the changing digital landscape that has emerged since its last revision in 2017. Through a renewed focus on risks, guidelines, process, technical requirements, management, assurance levels and security, privacy and equity, NIST hopes to provide an evolving document capable of meeting the challenges and opportunities of digital identity.

Opening remarks by **Dr Thomas Skordas,** Deputy Director-General for Communication Networks, Content and Technology, European Commission

Dr Thomas Skordas began his remarks with a broad overview of the various areas of EU-U.S. cooperation on emerging technologies and standardisation taking place through the TTC. Dr Skordas cited advances on 5G and 6G technology, quantum technologies and the Joint AI Roadmap, among others. From there, he described the EU's ongoing work to promote the use of electronic identities and trust services, and to facilitate their adoption by people and private companies in the EU. The EU has been particularly ambitious, hoping to provide 100 % of the EU public with an electronic wallet that will provide user-friendly digital identification for all – while focused on providing the highest levels of security and trustworthiness. Dr Skordas drew attention to how shared values underpin the transatlantic agenda, with both the EU and U.S. focused on privacy, security, civil liberties, equity, accessibility and liability as they shape their individual digital-identity ecosystems.

Introduction and stage setting for the workshop by **Anthony Quinn**, Team Lead, Office of Standards and Intellectual Property, International Trade Administration, U.S. Department of Commerce (TTC WG1 Co-Chair)

Co-Chair of TTC WG1 Anthony Quinn's remarks centred on the work carried out by WG1. He outlined three key pillars of work: information sharing, technology collaboration, and stakeholder engagement. On information sharing, Mr Quinn spotlighted the Strategic Standards Information (SSI) mechanism, which allows the EU and U.S. to share information on international standards and activities, and to facilitate coordinated action when necessary. Under technology collaboration, he stressed the importance of resource and information sharing in the realm of emerging technologies – despite historically diverging approaches. Lastly, he noted that the third pillar of stakeholder engagement is essential in supporting the objectives of the first two pillars due to the private nature of standards development on both sides of the Atlantic. In closing, Mr Quinn encouraged stakeholders to provide feedback to the TTC.

Introduction and stage setting for the workshop by **Thibaut Kleiner**, Director, Policy Strategy and Outreach, DG CNECT, European Commission (TTC WG1 Co-Chair)

Mr Kleiner, as Co-Chair of TTC WG1, opened his statement with the pivotal role that stakeholders play in standardisation – emphasising that while governments are there to set requirements, standards are developed by experts, companies and stakeholders that help shape and advance government activity. Digital identity has enormous potential for the digital economy and in boosting the digital transformation of the public sector, trade, industry and beyond. With the recent publication of the European Digital Identity Wallet, Mr Kleiner hopes that the tremendous potential of digital identity can be concretised through use cases.

Mr Kleiner also pointed to the importance of interoperability, echoing Mr Quinn's remarks on the historically different approaches of the EU and U.S. to standardisation. Focusing on interoperability is key to developing a global set of parameters and is the first step towards understanding the challenges and opportunities ahead for EU-U.S. cooperation. In a nod to Dr Locascio's opening remarks, Mr Kleiner underlined the importance of pre-standardisation research and innovation. Previous major successes achieved by WG1, such as the Joint AI Roadmap, should make the public optimistic about concrete outcomes on digital identity.

Initial statement by **Dimitrios Meritis**, Senior Advisor for International Science, Technology, and Innovation Policy, National Institute of Standards and Technology (NIST), U.S. Department of Commerce (TTC WG 1 Digital Identity Subgroup Co-Lead)

Co-Lead of the WG1 Digital Identity Subgroup, Mr Meritis, shed light on the work that has been undertaken by the European Commission and multiple U.S. government agencies over recent months towards better coordination on pre-standardisation research and innovation. Through monthly technical exchanges, the European Commission and U.S. government have been able to learn more about their approaches to digital identity in the hopes of developing a 'shared reality' of EU and U.S. regulatory environments, implementation nuances and future goals. Mr Meritis stressed the importance of transatlantic cooperation in pre-standardisation research. Despite differing approaches or regulations, EU and U.S. collaboration, along with robust stakeholder engagement, is a common objective essential to the success of the Digital Identity Subgroup, and to WG1 more broadly.

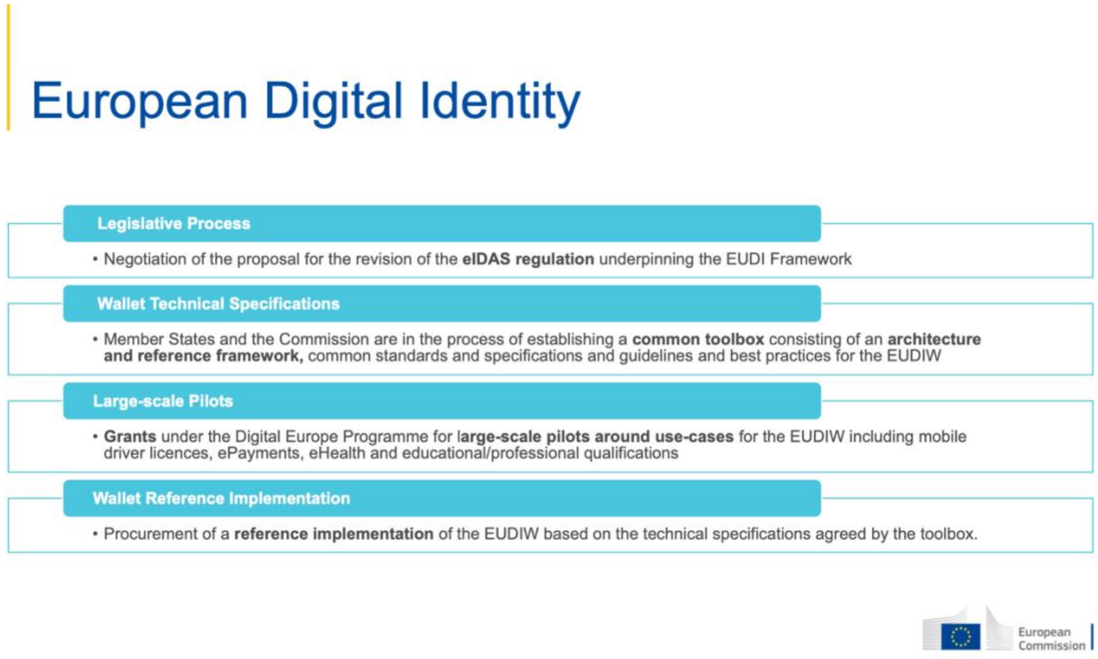
Initial statement by **Vicente Andreu Navarro**, Policy Officer, eGovernment and Trust, DG CNECT, European Commission (TTC WG 1 Digital Identity Subgroup Co-Lead)

Mr Andreu Navarro sought to delve into the necessity of developing cross-border interoperability between different jurisdictions with digital identity schemes. By beginning to interact early in process – at the technical level – like-minded countries such as those of the EU and the U.S. can begin to map out the challenges, opportunities and pending questions that will shape developments in digital identity on both sides of the Atlantic. In particular, Mr Andreu Navarro mentioned the mapping exercise planned by the EU and U.S. immediately preceding the and how it may mark a clear first step towards the technical convergence necessary for digital identity technologies. Central to this exercise are stakeholders, who can provide additional questions and answers on key use cases.

Presentation and Q&A session by **Paolo De Rosa**, Chief Technology Officer EUDIW, DG CNECT, European Commission on eIDAS 2.0 – 'Roadmap to eIDAS 2.0: A Discussion of the eIDAS Toolkit, the ARF and the Path to eIDAS Implementing Acts'

Paolo De Rosa presented eIDAS 2.0 and the broader concept of European digital identity. The idea behind digital identity is to provide access to public and private services alike by means of a EU digital identity wallet (EUDIW). The EU's vision is a voluntary digital identity that is free to the public, is accepted everywhere and is both secure and privacy-oriented – enabling people to remain in control of their data. To achieve this, four main streams of activities are taking place concurrently: a legislative process, wallet technical specifications, large-scale pilots and wallet reference implementation (see Table 1).

Table 1. Four streams of activity for European Digital Identity



European Digital Identity

Legislative Process

- Negotiation of the proposal for the revision of the **eIDAS regulation** underpinning the EUDI Framework

Wallet Technical Specifications

- Member States and the Commission are in the process of establishing a **common toolbox** consisting of an **architecture and reference framework,** common standards and specifications and guidelines and best practices for the EUDIW

Large-scale Pilots

- **Grants** under the Digital Europe Programme for **large-scale pilots around use-cases** for the EUDIW including mobile driver licences, ePayments, eHealth and educational/professional qualifications

Wallet Reference Implementation

- Procurement of a **reference implementation** of the EUDIW based on the technical specifications agreed by the toolbox.

European Commission

Source: Presentation by Paolo De Rosa, Chief Technology Officer EUDIW, DG CNECT, European Commission on 29 March 2023 at CEPS, Brussels.

After providing this high-level outline of the interconnected processes driving the development and implementation of European Digital Identity (EUDI), he presented some key use cases that will serve to provide both identity and functionality. This includes proof of identity, personal data control, proof of driver’s licence, the obtaining and presenting of medical prescriptions, and verification of social security status as well as loyalty cards, membership cards and tickets. There will also be a signature system for signing contracts and authorising payments.

These use cases then led into a description of the Architecture and Reference Framework (ARF). The ARF specifies the fundamental elements necessary for developing the EUDIW prototype, based on initial consensus among Member States. The ARF remains a moving target due to the ongoing legislative process and has been published via GitHub for comment.

Mr De Rosa said that while there are myriad use cases for the EUDIW, the two main use cases that have served as the basis for analysis of the prototype remain (i) a secure and privacy-oriented identification and authentication mechanism to access public and private services online; and (ii) a case enabling the user to obtain, store and present a digital document such as a driver’s licence.

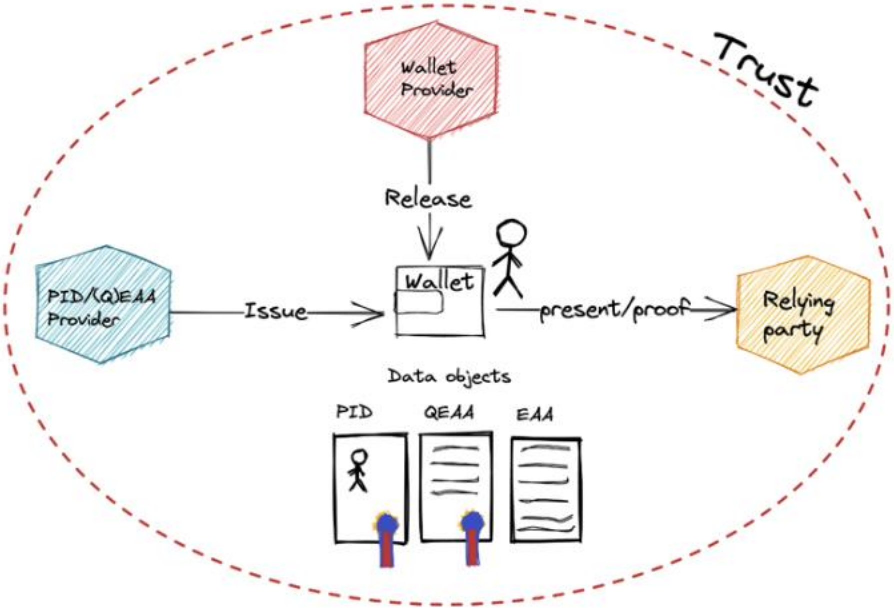
Importantly, the EUDIW is just one piece of a much broader ecosystem involved in the development of digital identity. At a basic level, this involves three main components:

(1) Governmental bodies will provide personal identification data (PID) and qualified electronic attestation of attributes (QEEA), such as digital education credentials, a digital driver's licence and digital travel credentials.

(2) The Wallet will receive, via the institutional provider and/or Wallet provider, the PID and QEEA. The Wallet is, crucially, held by the user, who then presents the documentation.

(3) The relying party will receive the information held by the Wallet and provided by the user. The relying party will then use the information to provide a specific service or do something for the user (see Figure 4).

Figure 4. EUDIW ecosystem



Source: Presentation by Paolo De Rosa, Chief Technology Officer EUDIW, DG CNECT, European Commission on 29 March 2023 at CEPS, Brussels.

This structure was reflected in the first release of the EUDIW technical specifications and brought to the fore multiple implementation challenges. Among these are storing cryptographic material and functions certifiable at a high level of assurance; developing a shared trust model among the different components of the EUIDW ecosystem; standardising (Q)EAA at the EU level and beyond; and ensuring a seamless user experience and broad adoption at the public level.

In approaching these challenges, the reference implementation is critical, as it will provide the technical infrastructure to support interoperability and implementation of the EUDIW and its broader ecosystem. Crucially, it will then be the reference as the European Commission supports Member States and other stakeholders in implementing and scaling up the EUDI framework. In an effort to construct this reference technical infrastructure, the European Commission has deployed four large-scale pilots with over 250 participants thus far. These multi-country pilots have brought in both the public and private sectors to test a variety of use cases, including among others electronic government services, educational credentials and professional qualifications, digital travel credentials, cross-country and cross-sector payments.

Mr De Rosa then answered questions as part of a stakeholder Q&A session.

Q&A session, *see Annex B.*

Presentation and Q&A session by **Ryan Galluzzo**, Identity Program Lead, Applied Cybersecurity Division, National Institute of Standards and Technology (NIST), U.S. Department of Commerce on SP 800-63-4 and what is next for digital identity.

Ryan Galluzzo first introduced NIST's digital identity programme, outlining NIST's cross-agency, multidimensional team – ranging from policymakers to cryptographers. It focuses on the development of certain core elements for the federal community, the international community and the commercial community to help advance digital identity.

The primary output from this digital identity team is the NIST *Digital Identity Guidelines*, Special Publication 800-63, which has recently undergone a fourth revision. At the level of the U.S. federal government, these guidelines are mandatory but they remain voluntary for any other entity. These guidelines lay out the process and system requirements for digital identity, covering such processes as risk management, assurances, level selection, identity verification and enrolment at different assurance levels, management of multifactor authentication, the issuing of credentials, exchange information between two trusted entities and more.

More broadly, NIST pursues both foundational and applied research. Through the TTC, NIST has largely concentrated on foundational research, which includes pre-standardisation research, with an emphasis on evaluating and understanding where the overall technology market is headed. The applied research takes place after the establishment of standards and aims to develop guidance and concrete capabilities for agencies or organisations that want to adopt and implement these standards. NIST also looks at metrology, and how this can be applied to identity to create more metrics and measurements.

The latest revision of Publication 800-63 came in response to the rapid social and technological changes that have occurred globally since the previous 2017 version. In the light of advances in digitalisation and the reckoning brought about by the Covid-19 pandemic, NIST's identity programme sought to centre security and inclusivity in the delivery of identity services. Starting from these two core principles, the updated 800-63 guidelines aim to emphasise optionality and choice for individuals; deter phishing, fraud and advanced threats; address lessons learned through real-world implementation; prioritise multi-disciplinary risk management processes; and clarify and consolidate existing requirements where needed.

This has resulted in a variety of important changes, with a select few highlighted by Mr Galluzzo. First, he addressed the revamped risk management and assurance selection process, for developing a framework and process that allows agencies and organisations to identify baseline assurance levels and then tailor it to meet the needs of both their organisation and their users. The new guidelines also include updated biometric performance requirements for proofing and authentication. These focus on responsibly deploying biometrics in identity proofing by ensuring greater controls and discussion around explicit consent for the capture of biometrics. They also include explicit notice to the end user about the uses of their biometric data, clear processes for how to manage, delete or remove the material, and greater transparency.

Publication 800-63 also introduces a digital evidence concept (e.g. the mobile driver's licence and verifiable credentials), which is one of the core areas of transatlantic cooperation. NIST seeks to learn from the European Commission's experience with eIDAS to better understand how digital components and digital evidence can be used in identity – particularly in these use cases where the EU has already taken steps towards pilot projects.

NIST has defined phishing resistance and updated password requirements in the new guidelines. The guidelines also mandate trusted referees and introduce applicant references. Trusted referees offer an attended process with a trained professional who can aid users who may not be able to complete automated proofing processes. Applicant References are individuals who can vouch for that end user's identity or attributes in a certain situation. Publication 800-63 establishes a new identity assurance level where biometrics are not required. Finally, in line with NIST's greater commitment to inclusion in the identity programme, the new guidelines provide normative language for the vendors and agencies to assess the impact of technology on equity.

After detailing the major changes included in Publication 800-63, Mr Galluzzo provided the audience with a broader picture of the research priorities of the NIST digital identity programme. He described

- accelerating the implementation and adoption of the mobile driver's licence (mDL) and user-controlled digital identities;
- expanding and enhancing biometric and identity measurement programmes;
- evaluating technologies that enable authoritative attribute validation;
- advancing secure, private, usable and equitable proofing and fraud mitigation options;
- speeding up the use of phishing-resistant, modern multi-factor authentication; and
- promoting greater federation & interoperability of identity solutions.

In closing, Mr Galluzzo discussed the importance of stakeholder engagement in shaping these draft guidelines. He asked for participants to comment on the *Digital Identity Guidelines* – which were open for comment through 14 April – and to provide feedback on the revised publication.

Q&A session, *see Annex B.*

Panel discussion: the relevance of transatlantic cooperation for different use cases

Moderator: Andrea Renda, Trade and Technology Dialogue

Speakers

- **Connie LaSalle**, Senior Technology Policy Advisor, Applied Cybersecurity Division, National Institute of Standards and Technology (NIST), U.S. Department of Commerce
- **Gudrun Stock**, Deputy Head of Unit, eGovernment and Trust, DG CNECT, European Commission
- **Herbert Leitold**, Executive Director, Secure Information Technology Center – Austria
- **Carmine Auletta**, Chief Innovation and Strategy Officer at InfoCert and Member of the Board of the Cloud Signature Consortium
- **Hannah Quay-de la Vallee**, Senior Technologist, Center for Democracy & Technology (CDT)
- **Julianna Cafik**, Principal Standards Architect, Microsoft

European Commission disclaimer

Legal process

The Commission notes that at the time of the workshop, the trilogues between the European Parliament, Council of the EU and the European Commission regarding the proposed European Digital Identity Wallet regulation were underway. As such, the Commission could not comment on the discussions in the ongoing legislative process.

Technical process

The Commission emphasised that the purpose of the event was to provide an opportunity to ask questions regarding the continuing cooperation between the EU and the U.S. in the context of digital identity.

In consideration of this event's general audience, the Commission noted that it may answer technical questions pertaining to digital identity developments within the EU and U.S. at a high level.

Introductory words by non-TTC participants & moderated discussion

Led by Andrea Renda, the moderated discussion spanned a series of high-level questions and recommendations from the non-government actors on the panel, followed by a Q&A session with the audience.

Introductions and panellists' role in digital identity

The panellists first introduced themselves and described the role they play in digital identity at their respective organisations and within the broader transatlantic ecosystem.

Introductions began with Herbert Leitold, Executive Director at the Secure Information Technology Centre in Austria. Beyond national digital-identity developments, he also works in the cooperation network on eIDAS and contributes to the European Digital Identity Wallet.

Mr Leitold was followed by Carmine Auletta, Chief Innovation and Strategy Officer at InfoCert, an identity provider under the successful and fast-developing Italian scheme on digital identity.

Joining online from the non-profit sector, Hannah Quay-de la Vallee, Senior Technologist at the Centre for Democracy and Technology, explained how she helps ensure that technology enables the support of digital rights, privacy and equity in both use and access.

Lastly, Juliana Cafik, Principal Standards Architect at Microsoft, described her work on applying governance to the identity ecosystem, while mitigating risk, and providing assurance for the security, integrity and usability of identity systems.

Discussion

Which use cases do you see as high value for transatlantic cooperation in digital identity?

Herbert Leitold pointed to use cases in travel services, mentioning car rentals as an example, where besides booking and paying for the vehicle online, one should also have the opportunity to prove digitally their ability to drive. In the area of civil aviation, the International Civil Aviation Organization (ICAO) is preparing an electronic pilot licence. Mr Leitold homed in on interoperability and its necessity for people, goods and services to travel.

Carmine Auletta raised the example of an EU-Japan proof of concept initiative, which used electronic seals that embedded local-entity identifiers, enabling Japanese companies to send invoices to companies in Europe. His example referred to the ever-growing EU-U.S. trade relations, which could benefit from such an initiative by making cooperation easier, less risky and more trustworthy.

Hannah Quay-de la Vallee brought the perspective of people, who could benefit from digitalisation of documents in their everyday lives. Beyond identification for movement and travel, she suggested that education and work certifications should be more transportable.

Juliana Cafik discussed the most critical use case from her perspective, in the financial sector: access to government benefits, services and high-value transactions. According to Ms Cafik, these should involve strong digital-identity ecosystems and alignment on foundational principles.

What is the most significant technical and/or policy challenge in the digital space?

Mr Leitold pointed to a critical policy challenge: shortcomings in applying the regulatory framework for mutual recognition of assigning liability upon errors in the digital space. He also raised the necessity of developing a common view and understanding of the concept of digital identity. Most obviously he referred to recognition of the identity of a natural person, but further agreements are needed on identities in transatlantic trade, the representation of legal persons, and objects or services. He emphasised that these aspects need to be addressed from the start, as otherwise, without clarity, obstacles will quickly appear.

Mr Auletta agreed that regulatory alignment is key, but technological challenges need to be addressed as well. He pointed to the partially failed example of the eIDAS 1.0, where the policy was clear from the regulatory point of view, but alignment on technical standards did not follow. This resulted in different approaches to implementation among Member States, leading to difficulties in making the identities interoperable. This is a lesson learned for the implementation of eIDAS 2.0.

Ms Quay-de la Vallee brought up the issue of equity. She said that it is oftentimes natural and necessary from a resource perspective to focus on primary use cases, which for digital identity are people who have regular access to smartphones, the internet and a standard residential address. This raises the conundrum of how to spread the benefits of a digital identity system to people who do not have such (consistent) access. This problem is further complicated when multiple jurisdictions and stakeholders are involved. From her perspective, one of the biggest challenges is how to make sure that adequate resources and time are dedicated to considering how non-standard use cases are supported.

Ms Cafik discussed technical hurdles, and time-sensitive and critical issues such as verifiability. She called for technical alignment on open standards, the identification of missing formats, protocols and cryptography. She also called for exploring AI for enhanced protections and potentially building in integrity and authenticity. Building a stronger chain of trust could provide a solid foundation to move forward and serve as a basis for policy to be 'layered' upon the technical level.

What are the transatlantic gaps between the U.S. and EU in digital identity that need addressing?

Herbert Leitold first referred to the issue of mutual recognition, and the need to address the matching of concepts and systems in the various jurisdictions. As the eIDAS 2.0 system is based on state-issued, mandated e-IDs with state supervision, it is critical to ensure that jurisdictions match and apply trust across borders.

Carmine Auletta then pointed to the cultural gap between the two sides of the Atlantic. Historically, Europe has been more regulation-driven, and the U.S. more market-driven, resulting in different perspectives. While not claiming one is better, Mr Auletta argued that when it comes to civil rights and privacy, as examples, the regulatory approach is probably the right one. Therefore, it is important for the EU and U.S. to find a middle ground in their approaches to digital identity.

Hannah Quay-de la Valle built upon Mr Auletta's point, laying out the complex technical implementation details that arise from the market-driven framework of the U.S. An issue near to the Centre for Democracy & Technology is the U.S. lacking baseline, federal privacy legislation, which results in companies and implementers being forced to fill the gap. First, this creates a patchwork approach. Second, it means that some, but not all, of the systems are adequately, technically set up to offer the kind of access that the European regulatory framework might favour. Specifically, companies cannot maintain certain kinds of data and therefore cannot be asked for access to such data by law enforcement. In conclusion, if an identity provider is managing privacy on their end, without any regulatory framework, it will likely not match up with the requirements of other regulatory frameworks. This situation, highlighted by Ms Quay-de la Vallee, leads to a significant gap that ought to be addressed.

Juliana Cafik shifted the conversation towards the perspective of the implementer. She claimed that there could be incredible opportunities for alignment in some specific areas, such as levels of assurance. She also brought up the importance of taxonomy, agreeing upon a definition of a relying party, for example. Creating shared definitions would help the implementers apply the regulation and the guidance appropriately and ensure they can embed the necessary measures from a technical security perspective. From there, equitable access, privacy protection and other issues could also be addressed. Overall, Ms Cafik argued in favour of simplifying measures for implementers to meet the regulations and correctly apply guidance.

European Commission and NIST interventions

The panellists' interventions were then complemented by government perspectives provided by Gudrun Stock, Deputy Head of Unit at DG CNECT, European Commission, and Connie LaSalle, Senior Technology Policy Advisor at NIST.

Connie LaSalle expressed her appreciation for everyone's contributions and engagement over the course of consultations and the current workshop. She noted that such active engagement could help to address the risk of a fragmented landscape of implementations of emerging digital identity capabilities, making workshops like the one in March all the more critical. Learning from early adopters across the Atlantic and elsewhere will be crucial to avoid this, particularly as NIST's process of standards coordination and guidance development hinges on contributions from the public sector, industry, civil society, and academia. Ms LaSalle also acknowledged the importance of broad, inclusive engagement as a measure to help address the digital divide.

Gudrun Stock echoed Ms LaSalle's appreciation for such broad engagement. She highlighted the value of transatlantic cooperation for use cases of digital identity and the importance of addressing the related challenges. The lively discussion confirmed the relevance and value of the transatlantic work.

Ms Stock referred to already mentioned use cases, such as the mobile driver's licence, which could produce results in the short term, provided they are based on internationally recognised standards. As an example, she referred to the ISO standard for driving licences. She also made reference to the use cases of professional and academic records, which could be recognised with specific validation tools in place, and a separate, necessary proof of identity of the person presenting the credentials.

Ms Stock also discussed digital travel credentials, which are currently being tested by a European Commission-funded project. This is the world's first pilot of transatlantic digital travel credentials, involving IDEMIA, a consortium of Dutch ministries, Amsterdam Schiphol Airport and KLM Airlines. The pilot project for digital travel credentials is being conducted for a duration of 3 months on flights between Canada and the Netherlands.

She highlighted that the European Digital Identity Wallet will bring together the process of identification and authentication, with the possibility of sharing credentials based on trust and thus simplifying such transactions for both users and relying parties. More pilots will be launched shortly to test the wallets in a number of use cases. These experiences will provide lessons for countries outside the EU as well, and help enhance the technical architecture of the wallet and the prototype, integrating international standards to the extent possible.

Ms Stock also referred back to the issues discussed by the panel and stated that they are well-known by both the EU and United States. The mapping exercise to be conducted after this event between the Commission and NIST would entail discussions on definitions and levels of assurance.

Ms Stock concluded her intervention by saying that many use cases of digital identity are of global relevance, and therefore international interoperability and mutual recognition of e-ID with third countries will need to be addressed. She noted that the current eIDAS Regulation and the revised proposal only explicitly provides for mutual recognition of trust services, not of e-ID. Hence, for the time being it could work with an international agreement or under the new regulation via an implementing act to achieve this recognition of trust services. Mutual recognition of e-ID with third countries could be possible via an international agreement under Article 218 of the Treaty on the Functioning of the European Union. She recognised the complexity of the process, but also that it remained very much within the realm of possibility. Against the backdrop of the UNCITRAL Model Law and the OECD guidelines for the governance of digital identities, such cross-border interoperability between jurisdictions is possible.

In concluding, Ms Stock highlighted that this event and the interest it has garnered from participants on both sides of the Atlantic demonstrate the importance and stakes of digital identity, and the necessity of cooperation in its development.

Final panel remarks

Herbert Leitold: on technology and interoperability, international standards are key. There are low-hanging fruits, where concepts are similar – such as for the mobile driver's licence. Starting with these would enable later advances towards more complex challenges.

Carmine Auletta: we do everything online, and to use that safely, we need identity. Since the internet is not limited to one country, identity in the digital world can only be tackled with an effort like this, with several Member States; no single unit can solve it alone. The challenge I see coming is that more and more interaction on the web is among software agents, raising the question of am I sure that I am interacting with a real person and not an AI agent.

Hannah Quay-de la Vallee: such stakeholder engagements are really valuable; we all have a lens we are bringing to these discussions. The cross-Atlantic interaction, but also broadening that to bring in the various stakeholders that exist, can lead to a more robust product with more longevity to it.

Juliana Cafik: there is a big challenge with respect to verifiability. We all have digital identities right now – we just don't know who has them or what they are using them for. We need to address that issue and put our actual, authentic digital identity in the hands of the rightful holder and then solve the issue of the verifiability of that holder with their legitimate, authentic credential, as well as who they are presenting it to. Anything we can do to rally around that in a timely fashion to meet the EU's timelines, I think would be a good effort.

Closing remarks: European Commission and NIST

Mr Meritis and Mr Andreu Navarro returned to the stage to provide brief closing remarks on behalf of NIST and the European Commission. Mr Meritis thanked the TTD and praised the engagement of the audience – both online and in-person – and encouraged stakeholders to continue to reach out to the Subgroup. Mr Andreu Navarro echoed Mr Meritis's thanks to the organisers and the audience. He closed by adding that the difficult discussions of the panellists and participants today prove the interest and complexity of the topic at hand. He encouraged continued cooperation from both sides of the Atlantic in tackling these pressing questions.

Annexes

Annex A. Reference documents

National Institute of Standards and Technology (NIST): SP 800-63-4NIST Special Publication (SP) 800-63: Digital Identity Guidelines

European Commission: eIDAS Regulation and EU Digital Identity Wallet

Annex B. Q&A session with European Commission and U.S. government representatives

Presentation questions	
Questions for Paolo De Rosa, Chief Technology Officer EUDIW, DG CNECT, European Commission	
Question #	Questions
Question #1	Say I'm French and I'm visiting Munich for the beer festival. Will I be able to use my EU digital identity wallet to buy beer at the festival? And does that mean it requires … biometric proof that I am the person who owns that wallet? I could lend my ID to my little brother who's under 18.
Answer #1	• Regarding identity proof for payments, this will depend on the solution implemented by the bank, but it won't necessarily be the case. • If you are using your identity to purchase the beer, you will need a way to be recognised, and this is something that will be done with the two-factor authentication. For the payments, this won't be the case.
Question #2	How will marketing organisations interact with e-ID? How will legitimate interest remain effective with unique and centralised identification?
Answer #2	• I cannot answer on the marketing side. However, the releasing of the identity is going to be done by an authority that is able to identify the person. But then, once you have the identity, it's [no longer] centralised. You will have your identity; you can use it … everywhere. Nobody from the central side will know if you're using that identity or not, so it's not going to be centralised.
Question #3	I would like to ask a question about the future certification of the wallet, the reference implementation or this prototype. Is it going to

	be by any means certified so that all the participating countries and other entities will be able to try a certified wallet? Or is it going to be an ongoing procedure, simultaneously [with] the implementation of the large-scale pilots?
Answer #3	• There is a certification process ongoing, mainly under ENISA. This is going to … also … involve the expert group and all the Member States; this will take time. • The requirements of certifications are going to be developed by a different agency and the expert group – that will start soon. To some extent it has started already. • The reference implementation should be able to be certified. Then certification has other processes in terms of operation. So you cannot certify necessarily only the software, you need to certify the whole solution and that will be in the implementation phase. It's not enough for the code to be certified.
Question #4	You identified four challenges. Do you agree that maybe there is a fifth that's on the right-hand side of the equation – the relying parties? Because it's not only the user experience and the user acceptance, but also the relying party's acceptance. The more difficult it will be to register or to authenticate as [a] relying party, the requirements you have to meet, which attributes you can or cannot use based on national law … so if it will be too difficult, do you agree that maybe [your] relying parties [might] say no, that's not something for me?
Answer #4	• That is definitely [a] challenge and not the only one; I agree with the issue raised. However, this challenge won't be any more complicated than the ones we are dealing with right now. • The relying parties today are dealing with this by asking, collecting such information directly from the user.

	• There will be integration tasks to be done. In the eIDAS implementation we saw limitations, especially in the public sector where it is not as easy to move as with businesses. • In conclusion, I do not see a lot of friction, because once the businesses … recognise the value, they will put in the effort.
Question #5	**Will the wallet be usable on all kinds of mobile devices? If so, is this a trade-off in terms of security?**
Answer #5	This is very good question too. Yes and no; there are currently three different architectures envisioned: (1) storing the crypto materials, the secret keys in the device; (2) storing the information on a smart card, like existing ID cards; (3) managing through a remote HSM, a specific hardware security module. The idea is to have a hybrid solution of this architecture exactly to answer … these questions, as we are aware that not all devices will be able in terms of security and certification to store this information in the device. For this reason, we envision that there will be different architecture that will allow the use of any device. But it's too early to try to properly [answer] this question, [yet] obviously it should be tackled in this way. We know that for years we will not have enough ready devices to store this information only within [them].

Questions for Ryan Galluzzo, Identity Program Lead, Applied Cybersecurity Division, National Institute of Standards and Technology (NIST), U.S. Department of Commerce	
Question #6	In your revision, did you look at other international, European, Asian standards or experiences? Because we are [at] a transatlantic interoperability event, and that would be helpful.
Answer #6	Yes, we do very much look at other international standards, other things that are going on and attempt to bring in and tailor things that are of value to us. We specifically reviewed: • Implementing Act • Good Practice Guide, UK • Pan-Canadian Trust Framework • ISO Standards 29115:2013; 29003:2018 We've done mappings to help evaluate whether there are lessons we can learn. The Revision 3 update was influenced by a lot of the work that was done, in particular in the UK.
Question #7	Use of digital ID is broadly optional, but 20 U.S. states are legislating to require online age verification. Are you working on that, especially age estimation?
Answer #7	So, I can't say that we're doing anything on age estimation. One of the things we are looking at with the mobile driver's licence project is when we can use things like attributes that are stored on something such as a mobile driver's licence, or potentially in the future, verifiable credentials as a way to assert a selected set of attributes that are released by the user. One of them could be age.
Question #8	I have a question related to your point about the relying party side and how to ensure uptake and provide guidance on that and understand what the impediments are before you can actually get value out of a credential such as an mDL. Do you have any knowledge already to spill about what are the impediments or … main obstacles that relying parties face when they

	have to readjust or reconfigure their systems in order to be able to accept, for example, an mDL.
Answer #8	I can't say that we know exactly what all the barriers are. It is everything from just understanding what mobile driver's licences are, to how they can be leveraged, to understanding what the international standards do and do not cover. There is likely an educational component, as well as how … we integrate these things with some of the core technologies that a lot of organisations already use today. That is one of the focus areas of the NCCoE project, to identify what are those gaps. Ideally, we'd like to be able to hand relying parties the ability to say 'these are the steps 1-100 that I have to do to accept these, and here is the value in doing that for me and for my end users'.
Question #9	**Can the integrity effect [of] this identity standards compliance be improved with continuous integration testing or machine-readable docs like NIST OSCAL?**
Answer #9	This is a fantastic question. I believe the answer is probably yes. We are working with our OSCAL team, having some initial conversations to understand when Revision 4 is done, what can we do. We have conformance criteria that we developed for Revision 3 and we are going to do it for Revision 4. But how can we take it to the next step and make some of these things a bit more consumable for different kinds of tools, for [the] actual kind of automation of your configuration and testing, for compliance? We are very much aware of this, and it is a long-term goal. First, the revision needs to be finished, and we hope to get to that point eventually with 800-63 and maybe some of the other documents we do as well.
Question #10	**One addition to getting into interoperability on a global scale is to use or leverage open source. What's your view?**
Answer #10	We are very much interested in exploring where open standards, in particular, can contribute to the deployment and development of these kinds of credentials.

	We are trying to understand where all of these things are going fit in together. We are aware of the Open Wallet Foundation. We are starting mDL because we want to understand that. It is key for us because we don't have many other forms of identification in the United States.

Annex C. Q&A with panel discussion

Panel questions	
Questions for panellists	
Question #	Questions
Question #1	euCONSENT works on interoperable age assurance. It seems to me that this is a use case which is somewhat neglected and is not one of the large-scale pilot implementations on eIDAS. It is not being studied by NIST. Digital identity is broadly optional, yet there are a lot of legal requirements: 20 states were mentioned earlier [that] are passing laws about age requirements, [the] GDPR Audiovisual Media Services [and] Digital Services Act. Do we think we are overlooking age verification and assurance?
Answer #1	Connie LaSalle: [the] short answer is no. NIST is addressing the topic, but using a different language, taking a cross-sector approach. But ultimately, the outputs of the research (presented by Ryan Galluzzo), and efforts supported through TTC play a role in this. I think general approaches to assertion from a protocol or policy perspective are covered. I encourage flexibility in terms of the taxonomy and lexicon. Gudrun Stock: the wallet can provide age verification. It might not be among the first use cases, but there are different technical ways to provide age verification. Paolo De Rosa: it is one of the most cited use cases when we talk about selective disclosure; therefore, it will not be forgotten. I am quite sure it will be covered in many situations.
Question #2	Since the digital identity requires different transactions with different agents at the same time, are real-time, latency, time-sensitive networks an issue in this regard or not?
Answer #2	Herbert Leitold: it can be an issue, but it has not been discussed in detail for the moment in the EU Wallet. Scalability is a related issue, and we have had a discussion with Paolo on how the concept could work on that. I am not sure whether latency in terms of

	authentication, when there is a human actor involved in the process, is that much of a concern – at least it has not been discussed that much so far. Hannah Quay-de la Vallee: latency to me also seems like an equity issue. Access to fast internet is a huge issue for rural communities. Therefore, this ties back to making sure you are thinking about who is getting left behind. I agree that it is not the most significant use case, if you have a human actor in the picture, that is the bigger challenge. But such technical implementation questions do tend to fall on equity lines, at least in the U.S. Juliana Cafik: with respect to the technical side of latency, it can be addressed in the implementation and the testing; therefore, I think it comes after the architectural details are worked through, from the wallet perspective.
Question #3	**Will software agents like IoT devices have a wallet?**
Answer #3	Gudrun Stock: not according to the current text.
Question #4	**Do you consider it compatible with human rights that all the digital identity infrastructure created at the national level is under the control of intelligence services? For example, in Romania all the registration adopted so far on the national interoperability platform states that the data collection infrastructure is managed by the intelligence services. However, the legislation does not have any rules [for] or control of this governmental agency. In this situation can this be considered dangerous?**
Answer #4	Hannah Quay-de la Vallee: there is real opportunity in the technical standards. Such convening, like the TTC, [is] incredibly valuable– to take mutually shared human rights values and think about how to embed them in standards, so that the technical framework enables the human rights even in a worst-case scenario. For instance (something that's already existing with mobile IDs), [design] them in a way that you can't necessarily follow an individual

	user based on when and where they're using their ID. As the technical standard, the way the mobile identity card is implemented simply does not allow for that. There are ways to embed what we consider human rights values into the technology itself. … The technical standards are a great way to build enough inertia value in the human rights standards that even bad actors who wanted to misuse them in these certain kinds of ways – whether that's government, whether that's corporate actors (which is something we worry a lot about in the U.S. as well) – simply cannot. These kinds of partnerships are a great way to start thinking about that and to embed those values early on, so that the technology carries them through – regardless of when or how or where they're being used. Juliana Cafik: this is a really important issue to tackle and often gets lost in the conversations around how … we technically interoperate and what are the issues of adhering to regulatory requirements where they apply. There are some foundational principles that need to underpin everything we do and those are the things that we should look to our North Star for identity ecosystems. Can they be baked into our architectures, into our technical designs? Can there be conformance criteria that implementers need to adhere to and can be assessed on, for equitable access, user control, sustainability, safety, privacy, freedom of choice and then underpinning all of that? Otherwise, they cannot be maintained. We can have those North Star goals, but they actually all have to be supported with a no-compromise approach to security. … That's how we have a level of assurance that those principles are applied and can be attested to. This is a really important conversation and it needs to be part of the conformance criteria and in the guidelines, exactly how … we apply this from a technical perspective.
Addition to Question #4	**Technical standards are not enough if the legislation does not give security and the possibility for the citizen to check what the**

	governmental agencies are doing. Moreover, [we need] to have a legal procedure in place for citizens to complain to the judiciary in defence of their rights if a governmental agency infringes upon them.
	Gudrun Stock: I think this goes a bit beyond digital identity as such, but there is always the possibility. I am not aware [of] whether in Romania the adoption of these laws [is] constitutional. It is possible also to see whether there is probably something in the laws that infringes upon the EU Charter of Fundamental Rights and there is a possibility to write to the Commission if citizens feel that there has been a violation of their fundamental rights in light of the EU Charter.
Question #5	The two sides of the Atlantic have fairly advanced economies, societies and safeguards. Might these digital solutions [be] a little bit more dangerous or … create even more problems if implemented elsewhere? … Digital solutions with infrastructure and services are potentially being deployed in third countries right through a task force that's in WG4. Do you have any idea so far on the future of digital identity solutions? I know that there are two pilots, [which are] going … to start in Jamaica and Kenya; [there] might be more but you know that's also from the TTC side.
Answer #5	Connie La Salle: I think we're open to it, but I don't know that formally. We've not done any cross-collaboration across working groups except for potentially outside … the context of the TTC. Yeah, but it's an interesting idea. I think I've viewed us [as taking] more of a crawl, walk, run, approach. [By] making sure we're laying some foundations and getting it right to begin with … then we can start complicating our lives a little bit more than they already are.
Question #6	We're in the middle of the negotiations on the eIDAS now. Should legislators have been involved in the TTC earlier, in the stage before it got to the point where we're in the last stage of negotiations? There are the initiatives from Senator Sinema, and House Representative Bill Foster [is] also [working on] digital identity legislation in the U.S. If there had been better cooperation between those [efforts] through the channel of TTC, maybe some of the problems might have been ironed out earlier in the draft legislation – and not left to have it … pick

	up the pieces or mend the problems afterwards. I'd be interested to know [whether] in the context of TTC in this particular example, … this is a sort of case study of when the engagement of legislators might have been helpful?
Answer #6	Connie La Salle: I think erring on the side of over-communicating usually doesn't hurt. I won't speculate, but in general, whether it's a legislative process or really any other policy development process NIST attempts to communicate its value, communicate its role, explaining why it's a non-regulatory body, why we see that as valuable and why we also see those who do have regulatory or policymaking authority as our partners with a very distinct role. So, I do think, you know, in the proposed legislation that you mentioned, there are elements of governance that could be helpful without getting into the content that NIST would hope to develop in a very open, transparent and collaborative way, with the people in this room. I can only speak to my experience within the U.S. domestic federal space, I won't speak to the state level [or] even more granular levels of policymaking. But I won't [blow] our own horn too much, [yet] I think NIST does a pretty good job of communicating our value and explaining where we see our roles and responsibilities lie. Gudrun Stock: I think it was more of a statement than a question and it's difficult to undo the past. To do it better would be great if it could be done, but I haven't found the way yet. So, I think we can only solve problems going forward.
Question #7	**Both the Commission and the Council [as well as] the Parliament are working with extremely ambitious timelines [in my view]… . I think you had a very interesting discussion about all the outstanding issues and the problems we face before we can have well-functioning digital identities and transatlantic cooperation. So, for NIST and perhaps also from a more technical point of view, Microsoft, how do you relate to those timelines? And do you have any objectives or ideas about where you see yourself and what you're aiming for?**
Answer #7	Connie LaSalle: well, I wish I had a crystal ball and I could tell you what the perfect timeline was. I think we can only do our best, map out

	dependencies and start working on them. I know at least on the NIST side we are a small but mighty organisation of government. We do our best to use themes like proportionality to figure out what the highest impact work would be for us to focus on and then we just start getting through it one piece at a time. The fact that we have this collaboration ongoing, I think is huge. It certainly helps us to flesh out which of those use cases are highest impact across more people than just what our focus might have been if we'd only focused on the U.S. So I'm already seeing the value of the partnership so far in that regard. Juliana Cafik: my contribution there would be again to align on open standards. And as a basis, ensure we actually land on agreement on those open standards, which are still moving at this moment in time. So, can the standards meet the timelines for the EU? That's the big question I have. And so the more effort we can put into locking down on those standards like mDL (or mobile driver’s licence) and VC interoperability profiles, files, formats and protocols for cryptography and so on, the better off we'll be in meeting that aggressive timeline. I think that that's really where the energy needs to go and with respect to this forum, I think my advice … would be more, more, please, more frequently. How do we help? We need to lean in this together. Tell us what we need to do. We're here. Let's roll up our sleeves and start to tackle some of these critical issues.
Question #8	**How is NIST working on the economic model around digital identity? It's a question that's been going around here in Europe: what is the economy behind the digital wallet? … I don't think I've seen any work from the NIST on that – is that a subject of discussion?**
	Connie LaSalle: interoperability is really important and making sure that we don't go from every user having 50 passwords to 50 wallets or even more credentials will let me know how valuable it ends up being. So, NIST sits within [the] U.S. Department of Commerce. We do partner with other components of the U.S. Department of Commerce who do that kind of economic analysis. But I think as far as a core competency of NIST, we recognise the market-driven approach that we have in the U.S. to work with. That's our reality and I fully expect that NIST will prioritise a set of research initiatives and our

	communities, whether they're commercial [or] academic, to join us and demonstrate to us where they see market value.

Annex D. Additional questions

Questions
1. How will marketing organisations interact with e-ID? How will legitimate interest (as a legal basis under the GDPR) remain effective with unique and centralised identification?
2. Could you describe how a French citizen would use an EUDI to prove their age to buy beer in Munich? Is biometric authentication required before it's used?
3. How is the wallet stored? On a physical device like a mobile phone? Is it maintained by the wallet provider (private industry) or a government service?
4. How will the selective disclosure of attributes (for instance from the PID to prove one's age of majority) be addressed?
5. Will the wallet be usable on all kinds of mobile devices? If so, is this a trade-off in terms of security level?
6. Will it be possible to verify certain attributes, such as age, anonymously?
7. How will interoperability with other jurisdictions, including the U.S., be achieved, particularly if the EU is proceeding first with development?
8. Of the countries currently in the pilot study, is there any consideration of African countries and future engagement of Africa on the digital wallets?
9. Online age assurance is not a large-scale pilot, but it is already a legal requirement under the GDPR, AV Directive, etc. Will the EUDI help a 13-year-old to access Twitter?
10. Will existing private-sector wallets provided by, e.g. Apple and Google, provide a challenge for customer uptake? What are the competitive advantages of the EUDIW?
11. Two of the four consortia you presented are using verifiable credentials, so they use the W3C VC. Which DLT are they using to check the credentials?
12. Use of digital ID is broadly optional, but 20 U.S. states are legislating to require online age verification. Are you working on that, especially age estimation?
13. Can the integrity and effectiveness of identity standards compliance be improved with continuous integration/testing or machine-readable docs like NIST's OSCAL?

14. What are the links between WG1 and WG5 on Data Governance and Technology Platforms?
15. It is compatible with human rights that all the digital identity infrastructure created at the national level is under the control of intelligence services?
16. Can I explain what is happening in Romania from a legislative point of view?
17. Since processing digital identity requires transactions between different agents, could the real-time interaction and latency be an issue?
18. Is national legislation that does not include real and concrete control of all the national agencies managing the digital identity system a danger?
19. How can we get involved in the mapping?
20. In my opinion, the most difficult aspect is to create a minimal data set e-ID or other data set, which is mostly constant.
21. Do you take into account in your work, for example, the OECD Recommendation on the Governance of Digital Identity?
22. With the EUDIW being developed as open source, could you see an avenue for states or the federal government to adopt/implement it?
23. How can we get involved on a regular basis? Will we be contacted from now on, having registered and participated in this workshop? How can we get involved in WG5?

About the TTD

The **Trade and Technology Dialogue** is designed to support the **EU-U.S. Trade and Technology Council**, which serves as a forum for the European Union and the United States to coordinate approaches to key global trade, economic and technology issues and to deepen transatlantic relations based on shared values.

Over a three-year period – from May 2022 until May 2025 – the Trade and Technology Dialogue will mobilise experts and stakeholders on both sides of the Atlantic with events and research outputs to facilitate inclusive, efficient and effective discussions and joint initiatives in support of the EU-U.S. Trade and Technology Council and its 10 working groups.

The Trade and Technology Dialogue is an EU-funded project, contracted to the Centre for European Policy Studies, the European University Institute, the Istituto Affari Internazionali, Forum Europe/Forum Global and the Providence Group.

We believe that stakeholders are a crucial resource to the success of the EU-U.S. Trade and Technology Council.

You can get in touch and learn more about the stakeholder activities and how you can contribute by regularly following the updates on Futurium, where all upcoming events, research outputs and further content will be announced (you can allow regular notifications in the settings of your Futurium account).

Sign up for the dedicated TTD Newsletter on Newsroom here.

For any other queries or for further information, email: info@tradeandtechdialogue.com

About the TTD Consortium

Consortium Leader

The Centre for European Policy Studies (CEPS) is a leading think tank and forum for debate on EU affairs, ranking among the top ten non-U.S. think tanks.

Consortium Partner

The European University Institute (EUI) is a doctoral and postdoctoral academic institution.

Consortium Partner

The Istituto Affari Internazionali (IAI), founded in 1965, is a private, independent non-profit think tank which promotes the understanding of international politics through research, training, conferences and publications.

Consortium Partner

Forum Europe's raison d'être is to bring stakeholders together to analyse, debate and inform policy making through the medium of events.

Capacity Providing Entity

The Providence Group provides strategic advice to transatlantic organisations in navigating the complexities of transatlantic data, privacy and cybersecurity risk.