EPFL

Center for Digital Trust

OBSERVER

Building trust in digital identities

Leveraging the power of technology, policy, and digital cooperation

Conference co-organized with

Geneva Internet Platform

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

C4DT Observer
#11 | July 2023

Foreword

Increasingly more governments around the world implement or explore the implementation of digital identity (e-ID) solutions, whereas regional organizations such as the European Union and African Union actively work toward fostering interoperability and facilitating the mutual recognition of e-ID solutions. Digital identities hold the promise of enabling economic inclusion and development, and of facilitating access to public services and to the reliable validation of credentials in e-commerce. In developing countries in particular, e-IDs are seen also as an important tool for promoting the UN's concept of 'identity for all' and for attaining sustainable development goals.

Yet, how can we ensure that digital identification systems are safe and trusted? How can interoperability, with that of portability, of national e-IDs across sectors and borders be accomplished? How can the highest levels of data security, privacy protection, and user-centered control over data be ensured? Who should develop, operate, and govern such a vital digital resource: the private or the public sector? And how can multilateral and multi-stakeholder dialogue and cooperation contribute to ensuring that digital IDs are indeed a force for good? These questions hold far-reaching implications for the economic viability, public acceptance, and societal impact of e-IDs.

Seeking to respond to the above questions, the conference "Building trust in digital identities – Leveraging the power of technology, policy, and digital cooperation" on 31 May 2023 in Geneva, Switzerland, brought together technologists, diplomats, policy-makers, industry experts, and the general public to discuss and exchange insights on digital identities and their effects.

This conference was jointly organized by the Center for Digital Trust (C4DT) at EPFL, the Swiss Federal School for Technology, the Geneva Internet Platform (GIP) and the Swiss Federal Department of Foreign Affairs (FDFA)

After an opening talk, during four thematic panels, panelists and participants explored the promises and challenges of e-IDs, gained an overview of the latest technological developments, discussed how to foster public trust in e-ID and beyond, and explored how digital cooperation and learning from each other can lead towards viable and trustworthy e-ID solutions. Importantly, the conference was also designed to not only facilitate exchanges among different stakeholder groups, but also among the representatives and discussants from different geographies, including in Switzerland, Estonia, South Africa, and India, as well as international actors such as the International Telecommunications Union (ITU), World Economic Forum (WEF), the International Organization for Standardization (ISO), United Nations Development Program (UNDP), World Bank and the Organisation for Economic Co-operation and Development (OECD).

This report summarizes the contributions and insights of our panelists, panel discussions and audience interactions. It was written with assistance of DiploGPT, a sophisticated, domain-specific artificial intelligence solution designed to exploit the capabilities of advanced natural language processing technologies. To learn more about DiploGPT, please visit DiploFoundation's AI page.

Opening session

Jean-Pierre Hubaux, academic director of the Center for Digital Trust (C4DT) and emeritus professor at EPFL, opened the conference with the observation that although the Internet is more than half a century old and machines have no problem identifying themselves, humans still struggle to establish online their proper, unique identities. He noted that achieving a proper online identity that is respectful of human rights yet enables people to safely access internet features is vital to empowering citizens and supporting global prosperity.

Jovan Kurbalija, executive director of the Diplo-Foundation and head of the Geneva Internet Platform (GIP), also welcomed the audience. He raised a number of critical issues, such as the tension between machines and humans, the difficulty of digitalizing highly political and symbolic concepts, such as identity and the risks of verifying votes and identities by using Google, Android, and Apple operating systems. Dr Kurbalija suggested the need to develop bottom-up AI in order to protect digital identities.

Imad Aad, technical collaborations lead at C4DT, began his introductory talk “From passports to smartphones: Understanding digital identities” by providing the necessary technical background for understanding digital identities and discussing their relevance for our digital lives. He then addressed the different types of digital identities, the various approaches to digital-identity implementation in different countries, the need for interoperability, the importance of user literacy, and the need for international cooperation. Dr Aad stressed that digital identities are a promising technology but need to be implemented at the right time and in the right way in order to be successful. Notably, he delved deep into the concept of self-sovereign identity (SSI), which provided the needed conceptual grounding for the thematic discussions during the subsequent panel sessions.

PANEL 1

Essential considerations for digital identity systems

Promises, challenges, and governance


Melanie Kolbe-Guyot


Alison Gillwald


Aiden Slavin


Emrys Shoemaker


Benjamin Welby

The first panel focused on addressing the potential benefits, challenges, and risks digital identity systems may entail in an international perspective. A particular emphasis was placed on identifying must-haves for strong legal and governance frameworks.

Melanie Kolbe-Guyot, policy lead at C4DT and moderator of the first panel, opened the session by highlighting the many potential benefits of digital identities, including enhanced governance and public-service delivery, streamlined administrative processes, greater government transparency and accountability, as well as fraud prevention. This includes arguments for e-ID's potential for enhancing electoral processes, enabling economic and financial inclusion, and for promoting the UN concept of 'identity for all.' Dr Kolbe-Guyot also highlighted challenges related to the design, development, and implementation of digital identities, as well as the risks to human rights, in particular, in terms of privacy, freedom of expression (surveillance), and discrimination. She invited the panelists to share their perspectives on essential considerations for advancing digital-identity systems and on the need to develop the right legal and governance frameworks.

Alison Gillwald, executive director of Research ICT Africa, stressed the relevance of digital IDs for effective citizenship and economic engagement in the Global South. She cautioned that digital inequality — the divide between those who are connected and those who are not, as well as those who possess the means and skills to transact safely and those who do not — is an important context for considering any digital ID projects. She emphasized that, first and foremost, critical digital public infrastructures — regulated and treated as public goods — have to be accomplished before we can turn to broader questions about data privacy, security breaches, and the potential for surveillance in e-ID systems. Dr Gillwald highlighted the importance of the wider trust ecosystem: Trust in the digital system is essential and requires institutions and public frameworks that are public-interest focused, in particular the interoperability and data-policy frameworks. It is important that these are collectively derived, equitable, and fair.

Aiden Slavin, project lead of the Crypto Impact and Sustainability Accelerator at the World Economic Forum (WEF), discussed the technical, policy, and governance challenges associated with digital ID systems. Departing from the question about why favoured decentralized ID systems, for example SSI systems, have not yet realized their promise, Mr Slavin discussed potential barriers to the success of digital identities. These barriers comprise the following types: technical (e.g., scalability and user design), policy (e.g., a lack of alignment on principles of digital privacy, user centricity, and security), and governance and implementation (e.g., the risk of exclusion and the need for clear utility for everyday people). He suggested a trial-based and principles-based approach to digital-ID systems and highlighted the need to address the risks of data exploitation, re-identification, surveillance, tracking, and cyber theft.

Emrys Shoemaker, researcher at the Graduate Institute and senior advisor at Caribou Digital, discussed digital identity as a relational phenomenon: a fact that, according to Mr Shoemaker, needs to be considered as people interact with each other and digital systems. He raised the issue of inclusion as a main challenge from a design perspective. Mr Shoemaker highlighted the importance of governance — in particular, in regard to ensuring accountability, inclusion, and empowerment — for mitigating risks and maximizing opportunities of digital identity solutions. He shed light on the unique challenges and the risks posed by digital-ID systems for marginalized communities, such as migrants, in regard to access to benefits, potential discrimination, exclusion, and targeting. Mr Shoemaker concluded that it is important to seriously consider the potential implications of a particular digital identity or wallet design for vulnerable groups.

Finally, **Benjamin Welby**, policy analyst for Digital Government and Open Data at the OECD, rounded off the discussion by reflecting on the OECD's ongoing work on recommendations for the governance of digital identity. He argued that it is important to take a step back from technology considerations to also think about how to create the appropriate playing field for digital governance and digital identities to be successful. Mr Welby emphasized that digital identity needs to be understood as an enabling tool and should be designed with user-centered and inclusive systems in mind. It is important, he explained, to consider the broader context of digital-identity governance — including regulatory frameworks, data protection, and privacy — and the interoperability among countries. He affirmed that trust is essential to the success of digital identity initiatives and opt-out options should be available for those who choose to not use them.

Overall, the debate highlighted the importance of digital identities in economic, political, and social regards, and the need for thoughtful design and governance when implementing these systems. In order to ensure digital identities are used for their intended benefits, interoperability, trust, user literacy, inclusion, and opt-out options are needed. A prominent traversal issue emerged: For digital IDs to be effective, it is important to establish the necessary preconditions. This includes building digital trust in the broader digital ecosystem that comprises appropriate institutions, actors (outlining their roles and responsibilities) and regulatory frameworks. This also means ensuring that digital-identity initiatives do not exacerbate existing inequalities, for example, by establishing public good-driven digital public infrastructures and by pursuing inclusive user-centered design approaches.

PANEL 2

Building robust e-ID solutions

Privacy, security, and interoperability

Imad Aad

Peter Waggett

Siniša Matetić

Annett Laube-Rosenpflanzer

The second panel explored the issue of trust in digital identities from a technological standpoint, discussing state-of-the-art underlying technologies and approaches, and how technical compatibility can be achieved. It also sought to highlight practical concerns in implementation regards.

Imad Aad, technical collaborations lead at C4DT and moderator of the second panel, opened the discussion by asking whether SSI is indeed the "holy grail" of digital identities? He inquired about how much of the promising privacy properties of SSI are still research-based and how much is in fact ready for deployment? Dr Aad emphasized the importance of zero-knowledge proofs and data-minimization legislation in enhancing user privacy. He also advocated the important role of academia in digital-identity discussions: Academia needs to provide sound research in order to contribute good ideas for designing and implementing digital identities, and researchers need to be able to convey these ideas both to legal and political actors.

Peter Waggett, IBM director of the Hartree National Centre for Digital Innovation and committee chair at ISO, shared his experience chairing the ISO Committee SC17 in which members work on the building blocks of trust in digital activities. Dr Waggett further shared insights from his experience in advising on projects in the United Kingdom on how to use identification technology and implementations to ensure that the outcomes are ethical and fair. He discussed some of the current technical challenges in enabling the use of various

types of credentials and privacy-enhancing technologies, such as cancellable biometrics and fully homomorphic encryption that are seen as able to help to create more trust in digital identities.

Siniša Matetić, head of technology and portfolio development at Swiss Post, discussed the need for the digital transformation of services in order to enable the building of a strong trustworthy identity infrastructure. He emphasized the importance of security, privacy, and usability for ensuring the successful implementation of automatic ID systems. Swiss Post, he outlined, plays an important role in providing trustworthy services to the citizens of Switzerland while creating a balance between centralized and decentralized systems. In this context, Dr Matetić discussed Swiss Post's plans for their own digital identity system, (SwissID), a centralized, previously privately-owned, solution with over three million users. Despite past criticisms of Swiss Post's identity solutions, Dr Matetić does not see them as being tied to a particular technology; he highlighted that Swiss Post is working on expanding the capabilities of SwissID.

Annett Laube-Rosenpflanzer, professor and head of the Institute for Data Applications and Security (IDAS) at the Bern University of Applied Sciences, discussed the potential of SSI and its drawbacks. Existing classic identity systems, Prof. Laube-Rosenpflanzer argued, have the advantages of nice usability, security, and of established standards; but they also have a privacy issue, as all traffic goes through a central identity provider. SSI, Prof. Laube-Rosenpflanzer outlined, has the potential to fill this gap by introducing two main features: a decentralized storage and decoupling of issuance and the usage of the identity. However, SSI comes with many challenges, including being a relatively nascent technology with high levels of complexity, potential security risks, and substantial user-responsibility demands. She noted that we still have little knowledge about the way to correctly implement SSI's privacy properties and that much development and research are still needed.

Overall, this debate provided important insights, on a technical level, into the challenges and potential of digital identities. Trust is an important factor in digital identities, and the participants explored various ways to build trust within digital identities, including technological solutions and collaboration between public and private sector stakeholders, and with academia. It was agreed that SSI constitutes a promising technology for helping create trust in digital identities, but that there are many challenges that need to be addressed. Interoperability, the discussion showed, plays an important role in creating effective e-ID systems by enabling a two-way feedback between industry and standards, thus enabling practical insight into how systems work and ensuring that standards are applicable and adopted by industry. It was concluded that, at least in the short-run, to ensure secure, reliable, and easy-to-use services for customers, a balance between centralized and decentralized systems is necessary, along with privacy-enhancing technologies.

PANEL 3

Best practices in governance and stakeholder engagement

Fostering public trust in e-ID and beyond

Benjamin Welby

Marika Popp

Rolf Rauschenbach

Vladimir Vujovic

Anita Gurumurthy

During the third panel, experts from industry, government, and civil society, as well as different countries in Europe and beyond, discussed the issue of digital identity and the roles private and public sectors play in its implementation and adoption by citizens.

Benjamin Welby, policy analyst for Digital Government and Open Data at the OECD and moderator of the third panel, opened the discussion by asking about the role that governments can play in overseeing industry experts and in developing digital public infrastructure. He observed the importance of balancing the different agendas of governments, the need for digital societies, and the need to convince citizens of the usefulness of digital identities. Mr Welby noted that the private sector and civil society also play an important role in digital identity, and he suggested that open-source solutions and open standards are important for achieving its adoption. He also pointed to the necessity of trust and transparency in order to protect and restore trust in the event of problems with digital-identity implementation.

Marika Popp, head of sales and partnerships at Cybernetica from Estonia, reflected on lessons learned from Estonia's adoption of digital identities twenty years ago. In this context, she

emphasized the importance, when creating a digital identity framework, of understanding primary use-cases (i.e., meaningful sets of services) and the need for the involvement of the private sector in order to drive the meaningful demand for said framework. The financial sector has, for example, played a significant role in this. Ms Popp also highlighted the need for decentralization and transparency in digital-identity solutions. She cautioned, however, against considering open-source software in countries with limited capacity to maintain them. She affirmed the need to involve private sector entities in order to encourage the adoption and acceptance of e-IDs by the population. She lastly also highlighted the benefits of joining late the digital-identity game, as it provides the opportunity to avoid the mistakes of other countries.

Rolf Rauschenbach, communications officer at the Swiss Federal Office of Justice, discussed the current "honeymoon phase" of the Swiss e-ID project and the need to be open and transparent in testing and developing it. Reflecting on the Swiss experience so far, Dr Rauschenbach stated that an open, transparent, and participatory approach to stakeholders has proven to be productive. However, he noted that the main challenges are associated with the unique Swiss political system. Dr Rauschenbach also highlighted the importance of communicating use-cases to citizens and of proper public "branding" of digital-identity solutions — both are aspects that the Swiss government is currently actively engaged in.

Vladimir Vujovic, senior product manager at SICPA, discussed the importance of finding the right balance between openness and control in order for digital identity to be successful. Regulation, he stated, to encourage actors to become issuers and reliant parties, and to provide maximum value, should be designed in a way so that it is not too heavy or cumbersome. Mr Vujovic argued that open standards are key for achieving interoperability and cross-border functionality. He pointed out that to gain public trust, an e-ID system must be reliable, easy to use, usable across many contexts, and offer convincing use-cases for the citizens. He added that, to assure trust among the citizenry, such systems must also have procedures to follow, in case something goes wrong.

Anita Gurumurthy, founding member and executive director of IT for Change from India, outlined the role of India's national ID program, Aadhaar. Part of a bundle of digital public goods, known as India Stack, Aadhaar is a twelve-digit digital-identification number given to 1.3 billion people in India, thus enabling them to remotely authenticate transactions, receive digital records, and sign documents. Despite, or because, of the shortcomings of Aadhaar, she argued, India is now at a turning point that can enable meaningful action towards a needed robust data-protection framework. Ms Gurumurthy also discussed India's consent- management tool, DEPA. It enables better data management and facilitates access to services. But, it raises questions about data-fication, data minimalism, and the need for institutionalized independent regulators to ensure the provision of meaningful financial inclusion. Lastly, she mentioned India's modular open-source identity platform (MOSIP) and the ways it can serve as a global digital public good.

Overall, the speakers discussed the importance of open-source solutions and open standards for achieving their adoption and the need for governments to understand and clearly communicate the primary use-cases for digital identity and to encourage its use. It was noted that the private sector and civil society should play an important role in its development and that the trust of citizens must be gained in order for it to be successful. In short, the panelists, spanning experiences and insights from Switzerland, Estonia, and India, exchanged on the potential of digital identity and the role of governments in its implementation and acceptance.

PANEL 4

Leveraging digital cooperation on e-ID systems for sustainable development

Joining forces for a secure and inclusive digital future

Marco Lotti

Jonas Loetscher

Hani Eskandar

Vyjayanti Desai

The fourth panel focused on the challenges and opportunities of digital identity in developing countries; they concentrated on the role and approaches of international organizations, as well as on ways to facilitate international cooperation.

Marco Lotti, external relations and partnerships manager at the Geneva Internet Platform (GIP) and moderator of the last panel, opened the session by making a case for complementing the complex picture of governance of digital identities by also examining its international dimension. Of particular interest to him were the ways organizations cooperated with other institutions and approached the interplay between the customization of needs and the assurance of interoperability across borders. Mr Lotti observed that, though organizations have different approaches to tackling the issue of digital identity, they are nonetheless complementary to each other.

Jonas Loetscher, expert for digital transformation for the United Nations Development Program (UNDP), argued that taking an inclusive approach to digital identity is essential; he specifically focused on people who are marginalized when engaging stakeholders. He sees UNDP's approach to digital identity as broader than just proving a person's

identity online, in a range from birth to death and covering both foundational and functional identities. This also involves putting individuals at the center of the design process and paying attention to the importance of mobile authentication. Mr Loetscher pointed out that digital transformation projects need to be tailored to the country in question. For example, he discussed Mauritania's digital-identity project that was heavily customized due to the country's specific needs. He highlighted the need for open-source pilots for digital identity in order to enable people to test, try, and further assess the technology.

Hani Eskandar, head of the Digital Services Division at the International Telecommunication Union (ITU), discussed the importance of digital transformation and the need for investments in digital infrastructure in order to enable interoperability and reusability. He affirmed that, in their efforts towards digital transformation, international operations and countries should be supported in a way that is tailored to their specific needs and stages of development. Capacity building, Mr Eskandar argued, is a cross-cutting issue for any digital-transformation initiative, and digital ID systems should focus on driving use-cases such as voting, access to social benefits, and on eligibility checks for services. He also discussed the ITU supported GovStack initiative that seeks to break down digital infrastructure into components and to create working groups around those components.

Vyjayanti Desai, practice manager of Identification for Development (ID4D) at the World Bank, argued that the World Bank has been leading the agenda of identification, as well as digitizing payments (G2PX) for the last seven to eight years. Through its three pillars of support (thought leadership and analytics, country engagement, and global convening and platforms), the World Bank aims to enable a billion people with either new or improved ID credentials by 2030. Ms Desai pointed out that, to realize this agenda, they are engaged in global cooperation with development and donor partners, as well as recipient countries. She highlighted that an inclusive and trusted identification system is essential to enabling access to services and economic opportunities for people. According to Ms Desai, the largest use-cases of this agenda, outside of finance, include the delivery of social assistance, payments, and means to access healthcare.

Overall, the panel discussion revealed that collaboration and cooperation among stakeholders at local, regional, national, and international levels is necessary to ensure successful digital-identity programs. Different development organizations can collaborate to address various digital-transformation needs of countries by sharing good practices, principles, norms, and standards, while also focusing on digital public infrastructure development and providing capacity building across the board. In particular, capacity building and literacy, as well as ownership of technology, were identified as essential elements of successful digital-identity programs. Panelists agreed that interoperability must be maintained while still meeting the specific needs of the countries.

Concluding remarks

Benedikt Wechsler, ambassador and head of the Digitalization Division at the Swiss Federal Department of Foreign Affairs (FDFA), offered concluding remarks, drawing conclusions from the panelists' inputs throughout the afternoon. Ambassador Wechsler stressed that digital identity is an individual human right and a vital part of digital life. Digital infrastructure has become a fabric of our daily lives, and digital identity is the key access to this. He reminded the audience that the Nansen passport was the first internationally interoperable identity document created in a humanitarian emergency situation. Ambassador Wechsler also observed that discussions and cooperation on this issue could be further enhanced in Geneva and Switzerland. Although not a front runner when it comes to digital identity, Switzerland has a strong ecosystem of international organizations, initiatives and organizations dedicated to digitalization such as the Center for Digital Trust, the DiploFoundation or the Swiss Digital Initiative, as well world-renowned academic research institutions.

About

Center for Digital Trust
Housed at the Swiss Federal Institute of Technology Lausanne (EPFL, epfl.ch), the Center for Digital Trust (C4DT, c4dt.epfl.ch) brings together academy, industry, not-for profit organizations, civil society, and policy actors to collaborate, share insight, and to gain early access to trust-building technologies, relying on state-of-the-art research at EPFL. C4DT is supporting the public sector by acting as an expert and facilitating technology transfer, in domains such as privacy protection and security, democracy and humanitarian assistance and critical infrastructures.

Geneva Internet Platform
The Geneva Internet Platform (GIP), initiated by the Federal Department of Foreign Affairs (FDFA) and the Federal Office of Communications (OFCOM) of Switzerland in 2014, provides a neutral and inclusive space for digital-policy debates and is recognized by the majority of global actors as a platform where different views can be voiced. The GIP provides a neutral and inclusive space for policy discussions, undertakes digital policy monitoring and analysis, and provides capacity development. The GIP is operated by DiploFoundation.

Digitalization Division,
State Secretariat of the Swiss Foreign Ministry
Digital foreign policy is increasingly becoming a permanent feature in today's diplomacy. Recognizing its significance, Switzerland published in 2020 a digital foreign policy strategy focused on digital governance, prosperity and sustainable development, cybersecurity and digital self-determination. The Digitalization Division within the State Secretariat of the Swiss Foreign Ministry is tasked with implementing the strategy and harnessing the existing synergies in the field of digital policy and especially with strengthening international Geneva as a digital hub and as a global center for digital governance.