SIDI Summit Paris Event Summary

Sustainable and Interoperable Digital Identity (SIDI) Summit November 28, 2023

Publication: December 22, 2023
Draft 1.0

Contents

Contributors

All SIDI Hub attendees contributed to this document, but neither individuals nor their organization will be named as per Chatham House Rules.

We are grateful to the Rapporteurs and editors of this document for their efforts:

Gail Hodges (editor)
Debora Comparin (editor)
Dirk Balfantz
Heather Flanagan
Yiannis Theodorou
Ana Latibeaudiere
Damian Glover
Gil Bernabeu
Rolf Lindemann
Daniel Goldscheider
Mirko Mollik
Ethan Veneklasen
Oatunji Durodola
Chahine Hamila

1.0 Summary

1.1 Background

The Sustainable and Interoperable Digital Identity (SIDI) Summit, held in Paris November 28th, 2023, was convened with a critical mission: to navigate and address the complexities of digital identity interoperability in a world that is increasingly interconnected yet diverse in its regulatory and cultural landscapes. This Summit recognized the imperative need for a global consensus that not only facilitates seamless cross-border activities but also upholds the principles of privacy, security, and individual rights.

The origin of this effort was several nonprofits observing that countries are currently deploying digital identity programs that they are not on a convergence path to global interoperability. Since people and businesses cross borders, the full benefits of digital identity and the ability to mitigate risks cannot be achieved without global interoperability.

The importance of digital identity has grown exponentially, driven by the shift towards digital transactions in areas ranging from finance and healthcare to education and government services. The Summit's agenda was to establish a harmonious balance between the technological possibilities offered by digital identity and the ethical considerations surrounding their use. This included an emphasis on creating systems that are interoperable across various jurisdictions while respecting the unique legal and cultural nuances of each region.

As digital identity becomes a cornerstone in both the physical and virtual realms of international interaction, the Summit aimed to lay the groundwork for a coordinated global approach. This approach must prioritize inclusivity and accessibility, ensuring that digital identity systems do not marginalize any group but rather empower individuals to assert the identity credentials they have. The Summit brought together a diverse array of stakeholders, from government representatives to standards bodies and non-profit organizations, all united in the goal of crafting digital identity infrastructure that is as interoperable and secure as it is user-friendly.

In essence, the Summit was not just about tackling the technical challenges of creating technically interoperable digital identities but also about ensuring that the policies and operations facilitate interoperability as well. The ultimate objective of the Summit was to define what we need to achieve global interoperability for digital identity, paving the way for a future where digital identity is a facilitator of global connectivity and inclusivity.

At the conclusion of the Summit, 92% of participants voted “yes” in the Exit Poll that they believe this work needs to continue into 2024. As a result, Summit participant feedback on the most promising tactics discussed during the Summit will drive the 2024 SIDI strategy and Summit approach.

1.2 Human-centric approach

The Summit discussion was anchored in a “human-centric” approach, consistent with the principles in these foundational documents:

- **Everyone** everywhere has the right to recognition **everywhere** as a person before the law. (Article 6 of the Human Declaration for Human Rights 1946.)
- "Provide legal identity for all, **including birth registration**" (Sustainable Development Goal (SDG 16.9)
- "Ensure **universal access** for individuals, **free from discrimination" (**Principles of Identification for Sustainable Development, Principle #1)

These principles were woven throughout the discussion during the Summit, and they will continue to be the foundation of SIDI Hub efforts.

1.3 Who participated & sponsored

The Summit included 120 experts from different aspects of the global digital identity community. This group provided a good cross-section of voices for this first global conversation.

Several organizations were invited to the Summit but were unable to attend. Those organizations have all agreed to join the dissemination list to receive updates on the Summit and future events.

As part of the SIDI Hub ethos of inclusion, no one entity sponsored, developed, or facilitated the event. Four organizations sponsored the event: Global Platform, OpenID Foundation, and the Secure Identity Alliance/ OSIA who together with Comexposium (Trustech conference host) these organizations

contributed 125k€. These funds were primarily used to offset travel costs for lesser developed country participants, as well as catering and venue expenses. The planning and organization for the event was conducted by 17 non-profit, co-organizers, with a wide range of expert volunteers acting as facilitators and rapporteurs for the sessions. The sessions themselves were conducted using Chatham House rules, so no names or organizations are referenced in the notes unless explicitly permitted.

1.3 Benefits of Global Digital Identity

The benefits of digital identity are well documented and varied, which is why many countries have chosen to pursue domestic implementations of digital identity. One of the pre-reading documents for the Summit highlights many of these benefits, (see "Human-Centric Digital Identity: for Government Officials" in the Appendix.)

The benefits of global interoperability are less well documented. Two benefits discussed during the SIDI Summit:

- **Trusted online transactions across borders:** Improves users ease of asserting identity information online and simplifies the ability to accept them
- **Trusted in person transactions across borders:** Beyond using passports to cross the border, digital identity allows users assert their identity and simplifies the ability to accept them

In both cases users can present a wider range of credentials, leading to less friction and more privacy benefits while helping businesses to improve their user experiences and lowering operating costs and complexity.

In short, residents, business and governments are all "winners," while the greatest "losers" are the bad actors that seek to exploit the porous surface of our digital lives and businesses. The inverse trajectory that we are on where a porous digital identity surface benefits bad actors and disempowers people, and undermines local communities and national governments alike is unsustainable.

1.4 Barriers to Global Interoperability

There are many barriers to global interoperability, including:

- Domestic-first objectives on the part of governments in designing digital identity systems[1]
- Difficult to identify the requirements for international interoperability given the domestic contexts are different.
- The technical and legal challenges of international recognition of digital identities
- Difficult technical normalization, as no single standard, policy or trust framework is likely to lead for all
- The product layer is immature in its technical ability to conform to global policies at scale
- Uncertainty about delivery times, given standards can take years to develop as can technically interoperable deployments.
- Unclear benefits vs complexity to citizens, organization and governments

[1] National digital identity systems, as designed by governments, are primarily tailored to meet domestic needs. These systems often lack the scope and design considerations necessary for interoperability at a global scale. This presents a significant barrier when attempting to establish a new trust framework that enables seamless interaction between numerous digital identity systems worldwide. Therefore, the role of governments in digital identity becomes crucial in addressing these challenges and facilitating global interoperability.

- Missing oversight body and/or missing definition of roles for each participant in the ecosystem and the related business model(s)

Foremost among the challenges is the domestic-first nature of objectives defined by governments in digital identity, where national and/or local governments act as the issuer, relying party and regulator of digital identity credentials. Even in markets where private sector entities play material roles, the government typically issues the foundational documents of residency and identity. The Summit participants concluded that “international” interoperability is most likely built off of “domestic” models of digital identity. With the key exception of the EU (eIDAS 2.0 Digital Identity Wallet), most ecosystem participants are largely focused on domestic implementations. However, each country is developing systems that best serve their local populations, and they do not have the option of building towards global interoperability since such path has been defined.

In the current context of domestic sovereignty, it is highly unlikely that all countries will be willing to follow the same exact tech stack (combination of standards) or trust framework, especially if it originated with a single company, country or non-profit. However, the Summit participants are optimistic that a roadmap and approach that is designed by the community for the community can provide a path toward international interoperability.

1.5 Shared Approach to Solution Design

Prior to the Summit, the global conversation on digital identity interoperability was largely limited to a few standards bodies, non-profits, government stakeholders and multilateral experts. Now the Summit has served to bring global stakeholders towards a common understanding of the problem, we can think about a shared approach to solution design.

To build global digital identity infrastructure that serves 8 billion people and mitigates global threats (e.g. global financial crime, protect against AI deep fakes, and address the next “COVID-like” health crises) we need a strategy that progressively engages more stakeholders and allows collective progress against shared global tactics

The good news is that a concentrated effort by a modest number of people can set the course for global convergence and interoperability. The Summit participants agreed that technical interoperability is hard across different standards (it is hard enough when the standard is the same), but it can be done. The Summit participants in the morning technical track discussed several options. More diligence is required to develop and weigh options, and work through a decision-making process if the optimal choice is not inherently obvious.

However, aligning trust frameworks across jurisdictions was perceived by many participants to be the harder task of the two. Multilateral trade agreements amongst countries, private models (e.g., ICANN), and hybrid public/private models (e.g., GLEIF) may offer useful models to build from. Whatever mechanism is developed, the Summit participants believe that respecting domestic sovereignty and human-centric approaches will be central principles.

A single workshop was not expected to lead to a solution design. However, we did align on the problem, the tactics most likely to help us make progress, and we affirmed that the global community has the “will” to get it done.

1.7 Tactics for 2024

At the end of the Summit, we surveyed all the participants, and 92% believed we needed to continue the SIDI hub efforts into 2024. Of the 8 percent remaining, there were no votes for “no” only “maybe.” This robust consensus gives us the confidence to start planning an approach to 2024 that builds on the areas of consensus established in the room.

For example, we asked participants which tactics they thought we needed to pursue in 2024, and this is a brief summary of the leading tactics with “yes” statements:

- **Continued Engagement:** A strong preference for ongoing participation in SIDI HUB activities and virtual meetings. (84%)
- **Defining Interoperability Requirements**: Establishing a consensus on the minimum requirements necessary for digital identity interoperability. (79%)

- **Global Metrics and Standards**: Emphasizing the importance of shared global metrics (77%) and aligning standards bodies including actively inviting representatives from Lesser Developed Countries to volunteer (77%) and clarity on what organizations are doing what (71%)
- **Mapping Trust Frameworks**: Mapping trust frameworks across jurisdictions, whether that mapping is country led (e.g., multilateral trade agreements), private sector led (e.g., OIX DNA Report) or public and private sector led) (69%)
- **Cross-Border Use Cases**: Identifying and agreeing on “champion” use cases that can drive cross-border digital identity initiatives (71%) and then mapping use case to domestic and regional policy (61%)
- **Data Governance Clarity**: Seeking more clarity in cross-border data governance and certification processes. (68%)
- **Roadmap Development**: A call for a clear 2024 roadmap (65%) working towards a longer-term plan for the five years to 2030. (61%)
- **Financial Support**: Addressing the need for more financial assistance for deployment. (55%)

These tactics reflect a comprehensive approach to advancing global digital identity initiatives, focusing on collaboration, clear standards, and practical use cases. Taken individually, each tactic will likely require its own workstream and participants to deliver it, in some cases through existing forums and standards bodies, and in some cases via new SIDI Hub workstreams. We also anticipate that the work required will include both virtual aspects, and milestone events where the SIDI community needs to convene in person.

The audience consistently expressed their desire to have use cases to focus the global work. A review of the votes made by participants as they exited the venue confirmed that there is wide variation on the use cases, and so there is no obvious choice though a few do “bubble up” to the top like financial services, healthcare, travel, and student study abroad. Refer to page 47 for more information on the audience use case “votes.”

A few tactics had a more mixed response in the poll, with 50% agreeing that it would help to have a list of academic questions that the academic community could lead, a statement that all participants might “sign up” to support received only 35% yes votes, and only 31% thought that a GLEIF identifier is likely to be a useful tool outside of financial services transactions.

More highlights from the exit survey are provided in the Exit Poll results distributed alongside this report and posted at http://sidi-hub.community.

1.8 Transparency

This Summary and rapporteur session are intended to reflect the substance of the first SIDI Summit discussion. We seek to offer transparency on our discussions and findings while protecting the views of individuals and organizations given the Chatham House Rules under which these discussions were held. We seek to use these materials to both inform digital identity experts about the findings of the Summit, and offer public transparency on the intention, substance, and direction of this work. To be timely with the release of this Summary, which reflects the combined efforts of over 20 volunteers, we kindly request the reader's understanding for the inclusion of rough notes, and any spelling, grammatical or formatting that may impede the reader's understanding of the substance.

1.9 Terminology

For the purpose of this document, we define digital identity as per the OECD definition as follows:

> *Digital Identity: A set of electronically captured and stored attributes and/or credentials that can be used to prove a feature, quality, characteristic, or assertion about a user, and, when required, support the unique identification of that user.* (Recommendation of the Council on the Governance of Digital Identity [OECD/LEGAL/0491])

1.10. How to Get Involved

To join the dissemination list, please sign up at http://sidi-hub.community. We will share information on the 2024 strategy, workstreams, and events in this central location. In parallel, we expect the co-organizing non-profits and other participants to amplify the work of SIDI hub in their respective channels, to ensure the widest reach possible for the effort.

2.0. Rapporteur notes

2.1. Welcome

Advisor to the ministry of interior:

- Trust is paramount when digitizing society. Citizens need to be able to trust the new digitized society. Here's what we're doing to accomplish this in France:
- There's a project called "France Identity" - which is a government project; there are also private projects but will focus on the government project during the talk.
- Digital Identity needs to be secure because identity theft is a problem. There's reported cases, but also many unreported cases. One aspect of identity theft is account takeover.
- A key component of France Identity is a new id card. It has an NFC component, which can be read by a phone. There's no face recognition involved, which was very important for public trust.
- Uptake on the new govt ID card is still a bit slow, so we've also developed a software solution (apps for Android/iPhone). It's still in beta/test phase and will be made more widely available in 2024.
- Use cases for the app:
    - **offline**: digitize driver license, and use it for in-person encounters with, e.g., police. This will be the first use case of digital identity in France.
    - **online** voting (will come later): expectation is that this will increase participation in elections. There will be first uses of this (still in test/beta) during the election in May 2024.
- Also, France is participating in the POTENTIAL Large-scale pilot for the EU Digital Identity Wallet process; achieving interoperability is very important.

Member of parliament:

- The Olympic games are coming to Paris next summer. They are a big challenge, where we need to balance security and civil rights. Identity plays a big role, e.g., people have freedom to move around, but only certain people can access the Olympic Village.
- 1. Identity is important for online commerce: who bought what from whom?
- 2. Identity is important for governments who offer civic services.
- 3. Identity in future online spaces will be important to combat fraud and abuse.
- Identity must be a sovereign solution: the state provides identity, not a private company.
- Warning about solutions from Big Tech companies: if Big Tech companies provide identity instead of government, they will have additional power in addition to what they have today, but they're not democratically elected.
- That's why Europe has eIDAS. Some citizens are worried about mass surveillance as a result of this new regulation. It's not designed to enable mass surveillance, but we have to prove that to our citizens. If necessary, we have to refine the text of the regulation.

- Identity has to be interoperable. Let's go back to the Olympics, or events like that: how do we make sure that people coming in from other countries can use their digital passports, etc.? We don't want just one Wallet from one vendor - we need different technologies that interoperate. Open Source is good.
- We do need help from the private sector, who developed much of the underlying technology.

Co-Organizers Official kick-off:

- Governments from global north and south are represented here, as well as standardization orgs.
- The goal is to achieve global interoperability. Definition of interoperability: can I use my digital credentials whenever I want to?
- (OECD definition of digital identity is shown on screen)[2]
- (reminder of rules for the Summit, Chatham House rules, etc.)

Summary of pre-Summit survey:

- Lots of desire in the room to create a roadmap toward interoperable digital identity, to meet colleagues from across the world, etc.
- large consensus on achieving minimum requirements for digital identity interoperability: let's try to start working on this today

Introductory perspective from Global South:

- We need to focus on inclusion when designing digital identity; this is especially important for the global south; interoperability is very important.
- The global south has limited resources, and varying regulations: these can be challenges for a more inclusive digital future.
- Yet, this has the potential to affect a large number of people: one African nation has over 100M digital enrollments *today*.
- In summary, the Summit should strive to define an interoperability framework that focuses on inclusion; one that works for the global community

Quick facts/notes:

- mobile device penetration in the global south is still somewhat lower, some countries are still lacking good 4G coverage.
- let's take this Summit as a starting point to change the game for global interoperability.
- there are many experts in the room, representing different countries, at different stages in rollout of digital credentials.
- (reminder to make most of the day: be present, help facilitators, take exit poll)
- (people will have a chance to review notes before they're being published)
- It's up to us how far we'll get today

[2] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491

2.2 Strategy Track

2.2.1. Topic 1: Human Centric Digital Identity & Benefits for 8 Billion People

The meeting started with information on one NGO’s role and interest in digital identity as a key component in poverty reduction and economic development. This NGO values its experience in implementing identity programs across countries, emphasizing interoperability and legal reforms. A significant part of the discussion centers on the challenges and requirements for international recognition of digital IDs, including state ownership, data protection laws, trusted frameworks, and common standards.

Key use cases discussed include student mobility and the potential for cross-border digital identity systems. The importance of aligning digital identity systems with human rights agendas, as highlighted in a white paper, was emphasized, alongside the need for government-centric approaches to digital identity as per OECD recommendations.

The meeting also addressed the necessity of adapting to local contexts, particularly in Africa, where the focus is more on addressing basic identity access and inclusion issues within countries before considering global interoperability. Alternative identity systems, such as human introduction systems, were discussed, highlighting the complexity of identity management beyond official documents. The overall discussion reflects a nuanced understanding of digital identity, balancing technological innovation with legal, ethical, and local considerations.

Key points:
The meeting notes you've shared cover a comprehensive discussion on the role of digital identity in global development. Here are the critical highlights:

1. **One NGO's Interest in Identity and Their Value Add**: This NGO is interested in identification as a key element in reducing poverty and advancing economic development. Identity is seen as a 'missing middle' that binds various development aspects together. They approach this through a digital public infrastructure lens, emphasizing the necessity of interoperability. Their value comes from implementation experience in various countries, convening peer exchanges, and providing technical assistance and lending for identity programs. They work at all layers of identity infrastructure, including legal reforms.

2. **Challenges in Recognizing Digital IDs Internationally**: The discussion revolved around what it would take for countries to recognize each other's digital IDs. Key factors include state ownership of the platform, robust data protection laws, a trusted framework following good practices, shared technology, a common standard for identity proofing, and a strong foundational legal framework.

3. **Use Cases for Cross-Border Digital Identity**: Travel and international finance regulation were discussed as complicated use cases. Student mobility was highlighted as a potential area for practical implementation, with a suggestion to look at programs like Erasmus for inspiration.

4. **Governance and Legal Frameworks**: Issues around the governance of identity systems, particularly passports, were discussed. The necessity of a legal framework for authentication and verification was also highlighted.

5. **Human-centric Digital Identity**: The paper emphasizes that digital identity systems must align with human rights agendas, highlighting the importance of edge cases in ensuring humane identity systems and recommending adoption of OECD principles. Open question: can this Summit agree to focus on the OECD guidelines?

6. **OECD Recommendations**: Governments are central to creating inclusive, empowering digital identity systems. The focus should be on individuals not currently using digital services, with attention to their specific needs. There are questions about how to track countries that intend to follow and measure their progress. The implementation of recommendations requires government action and evaluation of success over time, possibly using metrics from a digital government index.

7. **Perspectives from an African NGO**: This NGO focuses on the specific needs and demands of its constituency. The primary challenges in Africa are access and inclusion within their borders, with a current focus on resolving basic issues before considering global interoperability.

8. **Global vs Local Contexts in Digital Identity**: There's a need to understand local contexts when discussing global interoperability. The concept of 'human-centric identity' is crucial, with a focus on inclusion and developing local roadmaps for identity systems. We also need to understand that part of the local context is the existence of alternative, unofficial systems used for identification. The meeting discussed alternatives to official identities, like human introduction systems, and the challenges of decoupling identity from nationality. The potential for digitizing such alternative systems was also explored.

These highlights reflect a complex and multifaceted approach to digital identity, balancing technological, legal, and human rights considerations with a specific emphasis on local contexts and needs.

Strategy session rough notes
Slide 23 (topics to cover)

Slide 24 (base assumptions)

Slide 25 (Topic 1 - Human Centric Digital Identity)
What a major multilateral does in the identity space and why they are interested:
- interested in identification. They do interventions in countries to reduce poverty, advance economic development, and identity is a “missing middle” gluing it all together.
- Digital public infrastructure lens - foundational, horizontal layers that countries build on.
- Interoperability is necessary for this paradigm to come about.
Where they add value
- comes from implementation experience in several countries
- Convening peer exchanges
- Technical assistance and lending to make these programs happen
They intervene at all layers of the stack, from helping create basic records to building on existing infrastructure to encourage innovation.
- including helping drive legal reform
Question for the room: What would it take for you to recognize the digital IDs issued in other countries?
- state ownership of the platform and governance in place that supports interest of both countries
- A very good data protection law that protects the data of the individual and allows the individual to know who is asking for its data
- A trusted framework; one that follows good practices
- Shared technology
- What has to be government issued? The technology? The governance? Both?
    - The governance at least has to be owned by the government.
    - The technology just needs to be held in standards we recognized
- a common standard for identity proofing
- A strong foundational document that feeds into the digital identity process
- A legal framework for authentication and verification
- 28 countries asked this question in 1996 when talking about interoperability of passports. Today, what elements of identity that are derived from a passport are lacking? Example: identity assurance is covered by ISO 1903 (???) for passports. Let’s not re-do it if it’s not necessary.
    - Mostly the issues raised are around governance. So, is there something wrong with the governance framework for passports? The accessibility of the passport

- What are the use cases we are trying to solve? It's hard to find a great use case outside of travel. What would be the most important to drive interoperable digital identity across borders?
- Use cases are absolutely necessary. Until you do something with identities, you can't see the deficiencies. Travel, international finance regulation, they are complicated use cases. Let's look at something different: student mobility. Students want to study at different schools. So what's missing? Institutional affiliation and combining the student id with their national id. Look at the Erasmus program and consider making it interoperable outside the Erasmus partners. It's not a heavily regulated field and could be practical to work with.
- Back to what's wrong with the passport: when the person is recognized, nothing really happens. What do we want to have happen when a person is recognized from another country? Identity matching, record matching to drive service provisioning? That should help answer what's missing.
- One use case is the edge case of people who do not have passports or who do not want to share their passports.

Slide 31 (white paper)
Key points from the paper:
- digital identity systems must be grounded in the human rights agenda.
- The UNDP has an excellent framework to help map the governance process to specific human right instruments.
- Edge cases are central to making sure our identity systems are humane.
- Strongly recommend leveraging the principles of the OECD principles as being a superset of all the models reviewed

Slide 42 Second Major Multilateral Organization
Governments need to be at the core if we want systems that focus on inclusion, empowerment, and that everyone can be identified and access public services. Governments should focus on individuals who are NOT using digital services today. What are their needs?

Want to hear about the relevance of the OECD recommendations? What can we do to improve them? How can we move from principles to actions?

How will adoption be tracked?
- When a recommendation is adopted, the secretariat must help governments take actions to implement the recommendations. They will be required to evaluate the success in 5 years' time.
- How can we measure progress? There is a digital government index that has elements that will be part of the metrics, but they are still trying to figure out everything they should measure and what problems they'll try to solve.

African Development Organization is governed by 48 African governments. The governance structure works with each government, assigns an ambassador bureau. They do not follow trends, they follow needs and demands of their constituency. After 15 years, they've found that

good ideas don't set the agenda. Removing obstacles and solving problems sets the agenda. For Digital Identity, what are the problems in Africa? It's not global interoperability; it's important but not high on the list. They are struggling with access and inclusion within their own borders; they need to solve in their own country before they put resources towards cross-border use cases. The basic issues need to be solved first.

Raising the issue now does help drive the best practices to make future implementations better, but it sets the stage for work in 5-10 years.

We need the agenda to be responsive to the needs of these growing countries. Example: they see a problem with under-18 services, parental consent issues, etc. These immediate agendas are driving their resources.

"Inspired by the OECD criteria" is a better framing than "measured against OECD criteria".

A better way to know whether individuals have a human centric identity?
- inclusion. If you don't have a national register, including the legal frameworks to support it, then that's a major gap in where they are. What is happening in Africa, they are finding alternatives to those "official" identities. Life still goes on, so they won't jump and join these new systems until there are lower barriers to entry.

If it is premature for Africa to lean too heavily towards global interoperability, what can the rest of the global community to meet those constituents where they are now? Do the technical standards body need to close gaps (noting they don't have participants that help them know what the requirements are)?
- The wisdom about digital identity doesn't really change around the world. What is different and difficult is that lack of capacity puts barriers for the global south to get from where they are today to where they need to be. The message keeps being "you need to be here" but we don't offer how to get there.
- No government in Africa talks about digital public infrastructure. Fostering trust and inclusion is more urgent than DPI.
- They don't need knowledge of the future, they need roadmaps. We need to help them build their own roadmaps, and roadmaps need to be local.

In the OECD recommendations, the preamble notes that you must understand the local national context. Not everyone thinks that global interoperability is important; it depends on the local context. Even in the EU, there are different views. We need to not lose the discussion, though, about global interoperability. Just put it in context with capacity.

The edge case problem hasn't been solved in the global north, either. Building a digital identity system that relies on pre-existing identity is still a problem if that pre-existing identity isn't good enough. The scale may be different, but everyone is grappling with it.

There are people using alternatives to digital identity. What are some examples? Can they be digitized?

- Human introduction system - e.g., village elder or headmaster of the school will attest to a person's identity
    - Some countries are exploring pilots that digitize introductions through trusted testimonies
- SIM card registration forces getting an ID, as does banking, but that's the friction driving the work for the alternatives.
- The issues closer to the borders are a bigger problem, but we won't talk about that. Having issues decoupling identity from nationality.

2.2.2. Topic 2: The Domestic & International Gaps we know are there

Scene setting questions:

1. *What does a country need (locally) to create a well-functioning and trusted DID ecosystem)?*

    - Enabling legislation
    - National strategy
    - Trust frameworks
    - Funding for DID – WB 2.2bn
    - DID expertise
    - Privacy concerns
    - Security concerns
    - CRVS infrastructure
    - Clarity on public vs private sector roles
    - Mobile phone / broadband coverage

2. *What's preventing local Digital ID ecosystems from being interoperable across borders)*
    - Lack of Government investment
    - Lack of Global Governance
    - Lack of compelling use cases
    - Lack of business incentives
    - Lack of technical expertise among policymakers
    - Lack of interoperable standards
    - Fragmentation of non profits / standards bodies.

Summary of discussion points:

- To effectively make progress on Global interoperability we need to be proactively and intentionally recognize the local context and concerns in each country. Social, cultural, regulatory, legal norms.
- We heard about lack of trust and suspicions around how neighboring countries may use data in the absence of a well implemented and monitored trust framework.
- **Policy:** Quite a few people touched on the complexity of overlaying the legal with technical interoperability, so tools and expertise are needed to help countries achieve that.
- When it comes to solution design: Legacy systems are often creating barriers and that theoretically starting from scratch may be more effective as a country can build the right

foundations in terms of reflecting good practices – but that's more aspirational than practical in most cases

- **Delivery**: Some people spoke about the need to focus on Use cases that are based on min data requirements and are less heavily regulated, rather than start with fully fledged ones that are likely to raise huge privacy concerns and potentially open pandora's box.
- Overall – bottom up must meet top-down efforts - local environments have to be taken into account rather than just paying lip service to them – the example of OSIA was mentioned where private sector has come together with several governments to reflect open standards

2.2.3. Topic 3: Existing Governance, operational tactics, and the minimum requirements for interoperability

Introduction – scene setting.

- The importance of looking at regulation as a tool when needed
- There needs to be an ongoing evaluative process in place to determine appropriate regulatory context, structure, purpose, and specific use cases need to be subject to testing prior to writing regulations, ideally.
- We need to analyze if regulations adapted due to extra-territorial provisions are going to be efficient. “one size fits all approach" vs regulations adapted to specific jurisdictions, context of use, and local use case adaptation is most typically necessary for the best results.
- Identity is local and there will be many appropriate configurations of identity – ID cards, phone apps, digital wallets – different standards, different operating models and different legal frameworks.
- Where do we need to co-operate, with whom and how?
- Impact of AI – the identity ecosystem will be impacted by AI regulation. We are in the pre-standards stage as there is still much we don’t know. How can identity ecosystem actors nurture and build an evaluative environment? What tests can we run to understand what AI impacts, use cases, and interfaces will be important?
- The need to gather data and create an evidentiary basis for what we are going to do.
- All stakeholders need to have a seat at the table. Developing countries should have leadership in conversations that affect them. Make sure that there is wide representation from Global South / Global North.
- Proposed analysis for each country to do and map how to get to where they want to go.
- **Mapping** of existing requirements, stakeholders socio-technical and contextual boundaries, normative practices, individual vs group privacy, technological proof of compliance, etc
- **Measuring** the collected data and analyzing the gap to the desired outcome.
- **Managing** the ecosystem: Look at standards, pre-standards and best practices that can help. Not every thing needs to be a standard, however, there should at least be an acknowledged best practice.
- Importance to define a national strategy with input from all stakeholders to ensure representation of all societal viewpoints. Importance of identifying gaps in each jurisdiction, legislation and coordination between entities that touch identity.
- There are different opportunities and options to achieve varying levels of interoperability – common standards, data exchange, mutual recognition of identity schemes, trade agreements, etc

Discussion.

Countries shared their individual experiences, where they are and what they are planning.

- Some countries are already working on legislation, trust frameworks and overall governance.
- Importance of aligning on principles and technical requirements, which in some cases may be outcome based not necessarily prescriptive. However, in some use cases and locations, prescriptive approaches are the choice of the local governments and the stakeholders. Approaches should be decided at a local, subnational and national levels, with plentiful inputs from local jurisdiction by the stakeholders.
- Importance of improving registration and coordination between government departments. Addressing barriers to the appropriate, safe, and legal collection of information (e.g. internet coverage gaps). Creating a foundational identity. Registration at birth is important so that is not dependent on people enrolling into it.
- Foundational building blocks for identity. While there are already best practices regarding sharing of different information types, there are local differences in approach. These should be respected, and discussions can center on how to refine and improve approaches, ensuring that the local customs are respected. There is a general consensus that data is important, and is required for evidence-based decisions. However, there is a commensurate consensus that data protection and security must accompany data uses, along with meaningful oversight and the provision of redress for people using the system. This is particularly true for systems with mandatory enrolment requirements.
- Importance of political support.
- Integration with existing sectoral structures at the regional, national, and subregional level is critical; this will include the basic sectors, financial, health, education, etc. as well as public and private sector. There will need to be a discussion in each jurisdiction about key sectors, as there are differences.(e.g. banks, telecoms). Most jurisdictions have a complex network of sectoral regulations with difficult interoperability of the regulations themselves.
- Data ecosystems and information flows need to be constructed in a way that protects civil liberties and human autonomy, and also facilitates core data functions. Both need to be present to allow for effective data functions across government stakeholders. Currently, there are multiple structures evolving at international, national and local levels to facilitate the safe and secure and privacy-protective use of data, including identity data. Open interfaces, open source programs may enable lower costs and efficiency. However, such approaches will need to be analyzed against the risks of information overcollection and information misuse

Stakeholders' discussion.

- Importance of member inclusion and making sure there is local context. Moving from principles to action – need for roadmaps.
- Stakeholder engagement is an important element to define roadmaps and requirements.
    - Representation – different user groups, providers of services (including private sector), providers of technical solution, authenticators, international organizations
    - Timing – Stakeholder engagement after the fact doesn't work it has to start in the beginning and continue through – how do we solve this?
    - Trust – Trust between stakeholders (law enforcement / digital identity issuers)
        - Global barometer of trust - Survey on public trust in institutions – depending on the country who is trusted is very different. Private sector is often more trusted.
        - Law enforcement and national security access to identity data is a significant issue that can be a potent barrier to trust. Law enforcement should, as a best practice, not be the managers or controllers of identity ecosystems, and a best practice is to have strong legal guardrails around all access, especially law enforcement. A roster of historic exemplars has already provided ample use cases of how not to manage this access relationship. Strong and enforceable legal guardrails are a must in this setting.
    - Internal / external - Internal stakeholders first then civil society etc.
    - Civil society should be present at the very beginning of the conversation, and ideally there should be long-term involvement from civil society stakeholders at the local level in particular to assist in building trusted, non-adversarial and productive relationships.
- Data protection - Guardrails to ensure positive outcomes and beneficial uses of data are essential. Guardrails should also be locally relevant so as to prevent negative outcomes / inappropriate, illegal, or harmful use of identity data.
    - Minimize data collection - Data collection should only be based on the use cases you will need and if possible don't collect data that can later be weaponized.
    - Understanding the consequences of having data. What happens to a citizen if things go wrong? There are risks from governments, and also from outside threat actors. National cybersecurity risks for a country exist. There needs to be a mechanism for redress in identity systems, which is best articulated in regulation.
- Digital transformation to be looked at as a wider concept that includes digital identity and importance of looking at everything as a whole – digital and social inclusion is central.

- Importance of looking at regulation as a tool when needed and when no other alternative is possible (e.g., standard)
- When regulation is needed, we need to consider if one size fits all vs multiple jurisdictions – context of use and local adaptation is often required

- Identity is local and there will be many configurations of identity – ID cards, phone apps, digital wallets – different standards, different operating models and different law frameworks.
- Where do we need to co-operate, with whom and how?
- Impact of AI – identity ecosystem will be impacted by AI regulation. Pre-standards stage as there is still much we don't know. What tests can we run to understand what AI interfaces we will need?
- The need to gather data and create an evidentiary basis for what we are going to do. All stakeholders need to have a seat at the table. Make sure that there is wide representation from Global South / Global North.
- Proposed analysis for each country to do and map how to get to where they want to go
    - Mapping of requirements, stakeholders - Social and contextual boundaries, normal practices, individual vs group privacy, technological proof of compliance, etc.
    - Measure the collected data and analyze the gap to your desired outcome.
    - Look at standards, pre-standards and best practices that can help. Not every thing needs to be a standard
- Importance to define a national strategy from the top and bring everyone together. Importance of identifying gaps in each jurisdiction, legislation and coordination between entities that touch identity.
- There are different opportunities to achieve interoperability – common standards, data exchange, mutual recognition of identity schemes, trade agreements, etc.

Discussion.

Countries shared their individual experiences, where they are and what they are planning.

- Some countries already working on legislation, trust framework and overall governance.
- Importance on alignment on principles and technical requirements (outcome based not necessarily prescriptive)
- Importance of improving registration and coordination between government departments. Addressing barriers to collecting information (e.g., internet coverage gaps). Creating a foundational identity. Registration at birth so that is not dependent on people enrolling into it.
- Foundational building blocks for identity. Lack of best practice sharing and open available information on how well things work, which is required for evidence-based decisions.
- Importance of political support, integration with private sector (e.g., banks, telecoms)
- Integration of information in one place so that different services can use the attributes / information required as needed. With open interfaces, opens source programs to enable lower costs and efficiency.

Stakeholders' discussion.

- Importance of member inclusion and making sure there is local context. Moving from principles to action – need for roadmaps.
- Stakeholder engagement is an important element to define roadmaps and requirements.
    - Representation – different user groups, providers of services (including private sector), providers of technical solution, authenticators, international organizations

    - Timing – Stakeholder engagement after the fact doesn't work it has to start in the beginning and continue through – how do we solve this?
    - Trust – Trust between stakeholders (law enforcement / digital identity issuers)
        - Global barometer of trust - Survey on public trust in institutions – depending on the country who is trusted is very different. Private sector is often more trusted.
    - Internal / external - Internal stakeholders first then civil society etc.
- Data protection - Guardrails to prevent bad outcomes / bad use of identity data.
    - Minimize data collection - Data collection should only be based on the use cases you will need and if possible don't collect data that can later be weaponized.
    - Understanding the consequences of having data. What happens to a citizen if things go wrong? National cybersecurity risks for a country
- Digital transformation to be looked at as a wider concept that includes digital identity and importance of looking at everything as a whole – digital and social inclusion is important.

2.3 Technology Track

2.3.1. Topic 1 - How could interoperability be achieved?

The Tech Track began with an acknowledgement that interoperability is hard. For example, there are plenty of examples where OIDC implementations do not interoperate with each other. Often, this is due to the range of implementation choices available: if one OIDC implementation uses elliptic curve cryptography and another uses RSA, they will not interoperate. Other protocols suffer from similar challenges: this was true of SAML, and will be true of other protocols.

Complexity is another challenge. OID4VC is inherently more complex than OIDC, with more parties involved. This complexity and fragmentation impacts standards bodies, policymakers, issuers and verifiers. To address these challenges, interoperability needs to be achieved at policy, protocol and semantic levels. This does not mean diving deep into the inner workings of any protocol, or dictating which technology countries should use. Moreover, it's important to keep the needs of identity holders at the forefront of our thinking.

The pre-event survey indicates that signatures and credential formats are other important issues for us to work on.

Group discussion - Do we want bilateral or multilateral interoperability?

Arguments were put forward in support of both approaches. Proponents of bilateral interoperability felt that aiming for a Minimum Viable Solution is more realistic, as there are less parties, needs and systems to accommodate. One participant pointed to Trusted Traveler Programs as a relevant use case. These programs are typically enabled by bilateral agreements, for example between the US and countries like Canada and the Netherlands. Another example is data sharing between the EU and Ukraine, where it was not feasible to achieve a multilateral data protection arrangement quickly enough following the outbreak of the conflict, so a range of bilateral agreements were developed. Moreover, interoperability is often challenging even within a country, for example between different states and agencies in the US.

On the other hand, it was pointed out that people don't typically move or act bilaterally, but rather across many areas or trust domains. In the developing world there are regions and situations that require multilateral interoperability, e.g. anglophone versus francophone countries, or countries adopting different data regulations. By aiming for multilateral interoperability at a technical level, this allows for both multilateral and bilateral agreements at the policy level. TCP IP was cited as a comparable protocol that is fundamentally multilateral.

In conclusion, participants agreed that which approach to pursue (multi or bilateral) will be determined by the nature of the opportunity and associated constraints, with critical cross-border use cases a key driver. Some situations such as immigration and payments require multilateral interoperability. For other use cases such as refugees moving between two countries, or situations with heavy data protection requirements, a bilateral approach is appropriate. Another idea that received support was that there is a natural migration path from bilateral to multilateral interoperability, as facts on the ground change. For example, universities in a number of countries organized into national federations, which themselves subsequently organized into an international federation.

Options for protocol interoperability

The options identified before the meeting were harmonization of different protocols into a single protocol, asking issuers and verifiers to support multiple protocols, introducing proxies to enable data translation between protocols, or some combination of these approaches.

Looking at the eIDAS regulation, version 1 was based on a single protocol, SAML2, with each country running a node (Stock project). However, uptake was very low so this is not a good benchmark. The revised eIDAS regulation is predicated on a combination of harmonization (with a single core protocol, OID4VC, for remote authentication, and interoperability with external nations advanced via best practices and ETSI-mandated standards) and multi-protocol (two separate flavors of OID4VC are specified, one for issuance, one for presentation, plus mDL for proximity use cases).

The Ukraine case study was highlighted. Ukraine has requested interoperability with the EU in two areas: enabling qualified signatures from both geographies to be recognized (which is being achieved via the EU introducing a pointer in its trust list to the Ukraine trust list) and authentication (to enable Ukrainian citizens to access public services in certain EU member states.)

How might international interoperability at protocol and semantic levels be achieved?

The audience divided itself into five groups to discuss this, with each group playing back the key points from its discussion in plenary.

There was strong (but not universal) support for protocol harmonization, with proxies only used as a last resort due to the risk of increased complexity (one group proposed that some elements like signature validation could potentially be outsourced).

The harmonization process needs to take individual countries' requirements as key inputs, and countries should be given the opportunity to challenge the proposed interoperability architecture.

Initially, protocol harmonization should focus on consistent implementation of each model, federation and digital identity wallets, rather than trying to harmonize federation and wallets. A number of credential formats and multiple schemas are expected.

Implementations should focus on meeting minimum viable trust requirements — namely that the subject's identifier is resolvable, credentials are verifiable, the binding between subject and wallet can be validated, and protection of the user's data assured — and on sharing the minimum data needed to complete a transaction, while achieving a high level of security.

Ideally, interoperability between trust domains would be multilateral, however this was felt to be an unrealistic goal in the near term, for a number of reasons. First, we are not in a 'greenfield' situation, but one with a patchwork of existing infrastructure including differing mobile device and network capabilities. Also, the design of a multilateral system is likely to be very broad, which could cause challenges for external trust domains looking to interoperate.

Achieving semantic understanding between identity systems will be a key challenge. The first step is to identify the minimum elements that need to be expressed in order for two parties to come to an agreement in each specific use case, for example the context of where the identity is being used, required assurance level and other information needed to mitigate counterparty risk. This could happen in the context of a trust framework alignment exercise.

User experience is another critical consideration, which if neglected will likely result in poor or minimal uptake.

There also needs to be a way to renew or revoke trust agreements, as part of the measures to address security concerns.

Detailed notes

Do we want bilateral or multilateral interoperability?

- Envisage multilateral interoperability, as it's about people. People don't move bi-laterally, they move across many areas / trust domains.
- Bilateral first, leading to multilateral
- Some situations require multilateral interoperability (e.g., international travel), others require bilateral interoperability e.g. refugees moving from one country to another, situations with heavy data protection requirements
- Ukraine case study - not feasible to achieve a multilateral data protection arrangement in time, so had to develop 7 bilateral agreements

- In the developing world especially, there will be regions & situations that require multilateral interop, e.g anglophone vs francophone countries, countries adopting different data standards
- TCP IP was envisaged multilaterally
- Which answer (bi vs multi) is determined by the nature of the opportunity & associated constraints
- Focus it down and go for the minimum, don't boil the ocean
- Critical cross-border use cases are what will drive this
- US has multiple bilateral agreements for Trusted Traveller Programs e.g. Canada, NL, because interop needs to be negotiated between each country.
- Trade-off in complexity; to make something multilateral it has to work for everybody, sometimes it can't be boiled down to a common denominator
- The best model is multilateral, both from a use case and a tech standpoint. E.g., immigration, payments
- Even achieving interop between different agencies in the same country can be a challenge, e.g., between states within the US
- Interop is between a collection of services. Once 2 governments want to do business, interop will follow. Build on the availability of new technologies.
- Regardless of the use case, there are certain aspects that will need to be interoperable. We could start with those which are cross-cutting e.g., passports have standard information requirements.
- Higher education - universities in some countries organized themselves into federations, which subsequently organized into an international federation
- Multilateral is better in the long run as I only need to implement one solution, however in democracies we all want to be part of the decision process, takes time to respect each parties' needs, so bilateral is simpler. No one can predict what multilateral interop will look like
- On a technical level, aim for multilateral interop as it allows for both types of agreements (multi and bi-lateral) at the policy level

Protocol options for interoperability

1) Make them all the same (harmonization)
2) ask the parties to become multi-protocol
3) introduce proxies in between to allow for translation.
4) A combination of 1 to 3
5) Do nothing

Examples from eIDAS

- eIDAS1 - each country as a Node (Stock project) using SAML2
- V low take-up, low performance

- eIDAS2 - EUDI Wallet will use OID4VC for interoperability. 2 versions specified: Issuance and presentation. Also mDL for proximity use cases.
- eIDAS2 focuses on harmonization and multi-protocol
- Harmonization with countries the EU wants interop with is via best practices and standards (the latter governed by ETSI)
- Ukraine has requested interop in 2 areas: signatures (EU introduced a pointer to the Ukraine trust list, to enable qualified signatures from both geos to be recognized) and authentication (Ukrainian citizens can get access to certain EU members states' public services)

Activity - how does the audience think that international interop of protocol and semantic might be achieved?

Rapporteur's group

- A hybrid where you have proxies as a last resort; people here are focused on protocols. NIST approach is to accommodate everything due to many different contexts
- At transport protocol level it should be harmonized per model. At the top of the stack there you will need lots of credential formats etc.
- For semantics / schema it will be use-case specific, you won't get the world to agree what should be on a drivers license / uni diploma
- Agree more harmonization is better at the protocol level.
- Harmonization enables different protocols to be merged; if they come closer to a single solution versus proxies which could become more complex quicker
- Harmonization means you should be able to translate; a relying party should get what it needs to create an account. The relying party will ask for more / be more greedy (the Facebook approach); the system should focus on what's the minimum needed to create a transaction, otherwise you won't get adoption
- Agree with harmonization at the protocol level; if you start integrating systems via proxies it will get more complicated
- If everything is in the wallet, you have to trust the wallet; we don't want the wallet to be the arbiter of truth
- Create a balance between interop and security; don't make systems so interoperable that they become vulnerable; another reason to create interop at the protocol level
- If 2 systems need to communicate in a non-standard way, this can create risk
- It's possible to create a minimum threshold with high security levels
- What if a multi-lateral system is so broadly designed that it causes problems for other countries
- eIDAS is one wallet / one system; i have credentials that can hop between wallets and can build use cases; if the subject ID is resolvable and the VC is validatable, and also the binding between the user and the wallet; these are the minimum viable trust requirements

- Are we talking about federation or the wallet model? If one country starts with a federated model, another with a wallet model they won't be interoperable
- You need to decentralize to centralize better
- There is no universal federation for everything. E.g. in the US
- Simple user authentication is where federation is right now
- If you're vetted once and can connect to various federations
- Federation works via data flows via
- Interop should start
- Start with federation to federation and wallet to wallet' move to federation to wallet later
- Wallet breaks down into edge wallet and cloud wallet
- Proxies introduces another layer with additional actors
- Proxies will be there, but not to achieve interop
- Transport
- Wallet model - need to establish which parts need
- What's the difference between federation and cloud wallet?

Group 2

- We discussed protocols; agreed there are enough protocols, that's not the problem, it's the layer above that allows semantic understanding
- Talked about what are the elements that could be expressed for semantic understanding for 2 parties to come to an agreement
- Understanding the context of where the ID is being used
- Need to match assurance levels / cover counterparty risk
- Could we express a set of elements that could be expressed in a smart contract?

Group 3

- None of this matters unless you take UX into account
- How come I can make phone calls / send SMS anywhere in the world?
- Realized it's often a patchwork; you aim for harmonization / try to make it one thing but it doesn't quite work like that e.g. some using 3G, some 4G
- Do the patchwork, slide in some proxies to ensure there are systems people can use

Group 4

- No single solution / depends on the use case
- International research has had success in more towards harmonization
- Harmonization is the end goal; continue to develop bi-laterally & look for opps to harmonize
- What to harmonize? Each country to bring their requirements & challenge the model / look to converge
- Alignment to different trust frameworks
- How do different orgs trust each other?

- Security concerns - if we're moving towards harmonization, can't achieve this without security; within the trust model we need to continue to renew or revoke trust agreements

Next group

- Let's do everything needed to make it work
- If greenfield, go for harmonization, define one protocol, decide on a data model etc.
- But we're not in a greenfield / can't throw away everything we have
- Need to interoperate with what's out there
- Will need mutli-protocols and where these are not interoperable, will need proxies
- The reason eIDAS doesn't work with proxies is there's nowhere to sign into (problem with eIDAS1)
- If everyone accepts a credential, people will start using. eIDAS2 is not just about signing into gov services.

Additional notes from group discussion on Topic 2 (Rapporteur's group)

- Even on the edge, you are an endpoint, therefore identifiable; Protection of the user needs to be a by-product of the design
- The transport layer is key, as it's where I receive the information' can always outsource other parts e.g., signature validation to a third party
- Federation is an established method; The front end is where you can have the flexibility to have different personas, step up / step down e.g., "give me another credential"; can't do this with federation, you need to go back to the IDP
- Focus on minimum viable requirements, e.g. When we give refugees their first ID, we need to figure out where it needs to be validated; agree an ID that's acceptable to both CBP and Nigerian ID Management commission
- If a refugee comes to my country with no ID, I can generate a new ID, but only if I know no other country has issued an ID (otherwise there is risk of fraud); but a big privacy issue if we can some kind of API to validate this
- minimum components for interop depends on the use case e.g. for high scalability e.g. ioT devices where GDPR is not a problem, could be different
- Authentication and identification are the foundation + binding, user protection, non-duplication
- Why start from the wallet perspective
- E.g., to document a negative credential, proof of non-existence
- Needs to be agreement on profiles corresponding to different assurance levels e.g., 10 profiles that then need to be challenged a lot (e.g. you must use one of these 3 signature schemes, but you can be sure
- they are safe)
- Security - goes back to certification i.e. entities will certify a wallet / other components
- Signature algorithms can be part of the different assurance level profiles.

2.3.2. Topic 2 - Components

To set the scene, the facilitator introduces the Slide Global Interoperable Digital Identity. The Digital Identity Life Cycle covers different steps such as Registration - (identity proofing) Applicant, Issuance (Credential management), Identity authentication, Authorization, Identity management

e-passport is a successful example of an ID framework providing a international interoperability layer. This interoperability is based on:

- unique Governance (ICAO – members states)
- and one common, ISO-based technical environment (one logical data structure, one protocol, one signature [ICAO PKD])

Is important to note that biometrics used to bind the trusted, verifiable identity claims with the user presenting them has been added (in 1995) after the first deployments of the technology (in 1980)

Nevertheless, the e-passport doesn't offer all the expected features that a global ID standard should provide. some GAPS has been detailed such as

- designed for gov only
- one unique cross border use case
- one issuer per verifiable credential
- and by design no selective disclosure

it should be also noted that TRIP is a guidance only. some issuance rules may not be followed -> this is one raison that some country continue to issue visa

A second framework has been presented: the EU DI. Like the ePassport this ID framework is build based on a common, EU-defined technology (multiple formats, multiple protocols, multiple signatures [Member State trust lists])

Having multiple ID program raises another additional problem for global Interoperability described in the Interoperable trust slide:

- how to cross the boundaries between established eco systems?

[slide interoperable trust] TO allow different ID program to connect, you need to recreate/support the same rules defined within an eco-system (Trust, verification, …) with another ID program of find for each rules a equivalent

[slide Standards Interoperability] Looking global interoperability only with the lens of the protocols is not enough as a ID program is also an organization in place to operate the program , a complete system that off course use protocols

[slide encyclopedia of Identity standards] this is a tentative to create a mapping of all (600?) different standards currently available

ID is already supported by standards from ISO , country, EU, also in specific market specification tackle one part of the ID (interoperability, credential , data, ..)

After this introduction, the group split in different subgroup

the objective was to continue the first group effort by looking about pro and cons . For each option, what are the Key Components? which matter for interoperability? Does each option address challenges of both protocol and semantic? Can we disregard policy as a layer in the technical domain or does it need to be supported somehow?

- each group made a report to the technical community

group 1

This group had a very interesting discussion related to trust document, issuance, the attestations of the app

There is a need to define the different layers of the trust for Public and private entities

Different organization point are also important to allow cross ID project exchange – example the verifier needs to be certified / verified / audited in some case with similar levels

Other technical details may also have some importance example biometrics technologies may not be accepted by all different programs

Policy is very important to define the expectation.

One idea was suggested: define the structure of the Trust between ID program – all elements should be defined and for each element of trust you need to have the level of expectations

Group 2

The group was also excited by the level and interest of the discussion

Based on the first discussion (harmonization) this group try to detail the different component that compose the trust

then the group look about harmonization protocols and semantics

the group highlight that the semantic is important

the group discuss about proxy and agree that this may be useful to connect different deployment ID program or similar program with different maturity level. But this should be an intermediate solution

Evidence about trust and transparency in the issuing process is a critical point to create Trust

It has been noted that using different cryptographic mechanism may be simple to solve when country trust each other

Group 3

The group also have interesting discussion with heavy debate about global north and global south.

there are some important point to take into account . as an example how to defines interoperability rules with various environment: example deployment of smart phone vs feature phone, app vs browser , 5G vs 3G , etc.

Due to theses impact, one way may be to define a first level of interoperability to start with and that may set a basic interoperability level

the group also discuss about helping digitalization in the global south. As an example the definition of a model to “transform” plastic document to digital ID

the group also suggest focusing on use cases that may be deployed without strong digitalization level and the COVID vaccination proof was used as an example. This may be done by adding trust

group 4

Protection of the user should be within the design of the product / solution .

transport layer s key you can outsource signature validation but you need to ensure the transport of information

federation is a good framework, that can support multiple personas model and the evolution of use cases that may requires additional information.

there is may be an effort to have about minimum level of interoperability – this may allow to support specific use case such as refugee

the foundation of an ID program is authentication and identification with the binding mechanism to the end user

A good next step may be to define a set of profiles (-10?) that clarify the level of assurance and trust. This will allow to define all elements of trust and the associated certification/security requirements to help 2 ID program to set up trust

Key Definitions as used in SIDI Hub Summit 11/28/23.

2.3.3. Topic 3 - Key Gaps and Next Steps

1. Limited time left - so we skipped the “Key Gaps” topics and focused on “Next Steps”.
2. Focus on Next Steps
    a. How do we continue this discussion (working groups, code repositories, …), how do we collaborate together?
        i. Example 1: starting with technical exchanges on facts & interpretation of facts - to build trust among the participants
        ii. Example 2: special interest groups are often created in other alliances
        iii. We should share use cases - relevant example that help us learn more details
        iv. Question: What would help the global south to participate better?
            1. Cost is a major aspect, interoperability already is there to a certain degree. That has an impact on devices (smartphones vs. feature phones). Impact for trust and verification.
            2. Many technologies have been developed for the needs of developed countries and the markets there are saturated. Those technologies are pushed into markets of developing countries - but they are not fit for purpose.
            3. Inclusion is not a single step - it needs sustained efforts and support.
            4. Issues are: Limited resources and ideologies (once you have a card you are identified, but other country’s citizens might not internalize the relevance of such a card). Lack of knowledge. Global south has a different infrastructure environment.
            5. We should ensure we have participation from the global south in each working group.
        v. We need mechanisms to agree on outcomes and a joint understanding what success means.
        vi. We need more transparency on where the demand is. That might be quite different in developed and developing countries.
        vii. Open standards vs. open source - is not well understood.
            1. Open standards are a nice goal. In many countries proprietary solutions benefit the established players.
            2. Open source has now often become an entry point for proprietary vendors - providing essential add-ons to open source solutions. Open standards are the way to go to avoid vendor lock-in. Open source is sometimes challenging from a governance perspective.
            3. Mobile money works fine in the global south - it is based on established and standardized protocols. The challenge is not the protocol but the “trust center”.


SIDI
PARIS
2023

2.4.1.Trust Framework Analysis – Global Learnings

Speaker 1

In June 2021, the EU and US established the Trade and Technology Council (TTC) to promote transatlantic trade and investment in products and services of emerging technology, boosting innovation, and protecting and promoting critical and emerging technologies and infrastructure. Under Working Group 1 of the TTC is a subgroup dedicated to digital identity, which, over the last year, has collaborated through a series of technical exchanges, a public stakeholder event in March 2023, and a mapping exercise focused on comparison of the trust frameworks laid out in the 2014 EU eIDAS Regulation and NIST Special Publication 800-63, Revision 3. The rational was to start with stable documents whose timelines have allowed for the emergence of lessons learned from implementation, then conduct a similar exercise once eIDAS 2.0 and NIST SP 800-63, Revision 4 are final. In the coming months a report will be published with the results of the initial mapping exercise, which compares assurance levels, definitions, and international standards that are referenced across the two authoritative documents, accompanied by a period of public comment.

Futurium | Working Group 1 - Technology Standards - WG1 Digital Identity Subgroup Roundtable Workshop Report

On 29 March, a public workshop hosted by the Digital Identity Subgroup co-leads within the EU-U.S. Trade and Technology Council (TTC) Working Group 1…

futurium.ec.europa.eu

U.S.-EU Summit Statement | The White House

Towards a Renewed Transatlantic Partnership The United States and the European Union represent 780 million people who share democratic values and the largest economic relationship in the world. We have a chance and a responsibility to help people make a living and keep them safe and

secure, fight climate change, and stand up for democracy…

www.whitehouse.gov

A key finding: there are differences but also a lot we have in common.

There is consensus that such a mapping expertise could be useful for more countries

Speaker 2

OIX has done a comparative analysis of 8 trust frameworks. In this work 79 policy characteristics and 283 different values have been discovered. Thankfully there are few new characteristics emerging after the review of 8 trust frameworks.

The effort is driven by the idea that people will move through different trust frameworks. Some credentials remain useful while others don't in some target trust framework contexts. End Users will probably need some decision support when choosing credentials to present.

In some cases direct comparison of LOA between trust frameworks is possible, in many cases the underlying evidence used to achieve the origin LOA is more transferable to the target trust framework.

Speaker 3

The United Nations Commission on International Trade Law (UNCITRAL) plays a key role to establish a robust cross-border legal framework for the facilitation of international trade and investment. It does this by preparing a model law that can be adopted by member states regionally or unilaterally.

Harmonization won't work but a common language, common rules and laws (technical/legal/operational) will be possible. Moving to wallets there is a need for interoperability for digital identity to facilitate trade. Some smaller countries are interested to work together as they're stronger as a group.

We need standards for the payload and understand the provenance for different data in different jurisdictions. How do we achieve equivalence like we have with passports?

Asylum seekers might be willing to share more information than what my country is willing to share.

Visas are supplements as some governments may not trust passports and they act as authorization.

Many of these issues are general challenges in data sharing.

Biometrics and names can both change over time.

The Tony Blair institute for Global Change works with governments and political leaders and offers advice on how to transform ways of governing towards a Reimagined state. TBI supports leaders on Strategy, Policy and Delivery by leveraging Technology and leading technology partners.

This session focused on disseminating and discussing insights on the minimum requirements needed for the global south to facilitate interoperability of digital ID systems. There are four major differences:

- cultural and social norms
- technological maturity like basic mobile phone as opposed to smartphones
- regulatory environments are at different stages of development
- funding & expertise differs vastly (and therefore reliance on international aid etc)

Global convergence (interoperability or mutual recognition) with seamless functionality across borders is essential.

The audience ranked the minimum requirements needed as follows:

- Common standards
- Focus on ID inclusion first
- User centric Digital ID design
- Standardized data formats & authentication approaches
- Expertise & earmarked funding
- Privacy & Consent
- Alignment on TF roles
- Cross border use cases that drive demand
- Consistent Audits for TF Participants
- Affective dispute resolution

Members of the Global South need education about concepts like privacy and open standards as they focus on adopting new technologies.

2.4.2. Trust Framework Analysis – Taking Actions

[Summary created by ChatGPT from rough notes]

Global Governance Foundations and Outlook: The discussion focused on including the global south and understanding regional contexts. The complexity of identity in the digital age was acknowledged, with specific examples from Nigeria (advancing data protection), India (lack of privacy understanding), Thailand (regional sensitivity to privacy), and Africa (need for baseline privacy information).

Big Questions and Practical Tactics: The group pondered the meaning of privacy and emphasized the importance of consent, data sovereignty, and the need for Africa to have more control and return on investment. GDPR Article 40 was discussed as a model for personalizing data protection laws to specific regions, with mixed opinions on its global applicability.

Audience Interaction and Security Concerns: They asked the audience about audit processes and trust frameworks. Operational security gaps, social engineering threats, and the challenge of harmonizing processes globally were highlighted. The discussion stressed the need for collaboration between governments and businesses, and the existing trust framework in the banking sector was noted.

Automation and Standardization in Policy Implementation: The speaker addressed the divide between identity regulation and standard implementation. She noted the challenges in aligning government and private interpretations and implementations of standards. The need for harmonization in authentication and trust framework alignment was emphasized.

Audience Feedback: The audience provided insights on the internal challenges of understanding and implementing GDPR. They highlighted the difference between data protection and privacy protection and the impracticality of achieving interoperability across all use cases. The importance of practical implementation, risk reduction, and compliance was discussed.

Key takeaways include the need for more inclusive and context-sensitive approaches to global governance, the importance of understanding and educating about privacy and data sovereignty, the challenges in harmonizing global processes and standards, and the necessity of practical implementation and compliance in data protection and privacy.

Future Work

Potential future work may include:

- A robust conversation about how trust is impacted by government access to private sector data and public sector identity data.

- Local representative map, measure, and articulate their context, and conduct an evidence-based gap analysis for the local level first. This can assist short term deliverables of domestic

Rough Notes

The following rough notes are for reference for the summary.

Global Governance Foundations and Outlook

- tactics to include the south, we don't want any separation
- need to identify sub regional context
- Complex situation in the world with new technology in the space of identity
    - Inclusion of the global south
- (Nigeria): advanced data protection and privacy
    - want to update their old systems with data privacy
    - all identities in Africa should be treated equally
    - People need to be educated that their data belongs to them and not to the government
    - Privacy is prioritized on top, right after standards
- India
    - people did not understand privacy, some stakeholders thought they do not deserve it (or a different concept)
- Thailand
    - privacy is valued more, is regionally sensitive (not in terms of regulations, but by groups)
- Afrika
    - Need baseline information about privacy
- Big questions: what does privacy and data protection mean ?
    - We should ask them, not define it for them
    - Normative privacy and data protection principles already exist. However, there are variations by region and culture. OECD Privacy Guidelines articulate a core group of principles from the European perspective, See: OECD's Recommendation on Privacy (the Fair Information Practice Principles). There are additional principles growing from GDPR, and now GDPR + legislation. Togo is an example of GDPR + legislation, see: Law No. 2019-014 Relating to the Protection of Personal Data. Additional guidance comes from First Peoples, for example, Te Mana Raraunga, the Māori Data Sovereignty Network, https://www.temanararaunga.maori.nz. See also: First Nations Information

Governance Centre, *The First Nations Principles of OCAP,* https://fnigc.ca/ocap-training/ (establishes how First Nations' data and information will be collected, protected, used, or shared)
    - Consent is very important, by group or by individual, depending on cultural context.
- Data sovereignty is especially important in the developing world.
    - Afrika wants more control over data being extracted from the region, wants a return on investment.
- Audience is in consent with the feedback
- Practical tactics
    - GDPR Art. 40, a structure that can be used
        - Allows to personalize GDPR for a specific region
        - Adapt GDPR for the context
    - Mixed view in the audience if it works or not. However, there is a strong evidentiary basis that supports multi stakeholder codes of conduct that are created by local stakeholders, and adjudicated with fair procedures and oversight to ensure equality, inclusion, and non-dominance.
- [Do we need a global definition of privacy?] Privacy is deeply contextual.
- Regulator – Approved Codes of Conduct under Article 40 of GDPR are a legitimate way to contextualize use cases to a local context even when working with a near-globally installed set of regulations. There are now many such codes, and they are working very well.
- GDPR: it can be forced by law or used by the industry to improve processes
- How is enforcing GDPR outside of Europe?
- Some stakeholders articulated that their definition of privacy was "my data and how do I feel about it?"
- GDPR: how many people feel about my data
- A place of consent has to be there in favor of the person or the group of people, depending on context.

What does the audience think?

How does the audit process work
- a lot of optimism in the audience, but hard in practical

How to work with trust frameworks?
Move beyond the paperwork part is difficult
- attackers just do it to break the system
- a lot of attack vectors have to be considered (social engineering, etc.)
- Gap in operational security
- Good security need the theoretical and practical parties

Data is not good enough, put it into a QES, now it's good. Example from Germany
- Challenge in the country to harmonize processes, how will this be world wide?

We need to look wider: not only the governments talking with each other, but also business
Will governance build on the private sector work?

- Bureaucrats have the last word, but are happy from input from the private sector
- Challenge with market adoption: a lot of in production solutions work in different ways
- Focus und Trust and Interop will not be enough

Trust Framework are about risk minimization
Bank sector is the backbone of trust

- already used by the government and the private sector
- we don't have to reinvent the wheel

Communities need to come together to find a fitting solution
We are focusing a lot of technical comparison

- some tech problems need to be solved, but this is not all

Current solutions are sometimes a privacy disaster
Prior to adoption, proposed solutions need to be tested, and receive multi-stakeholder feedback. Regions and local contexts should be the ones to determine what works for them.
Decision makers need to who is privacy is implemented right now

- they need to talk with each other

COVID-19 was a wake- up call to most countries regarding the need to update processes

- the COVID-19ocertificate was used internationally for traveling
- TF: what does that mean, practical example
- Some countries forced people to get the certificate for authorized access
- A credential was issued to Mickey Mouse, with the risk to ban the root certificate of the whole country

We fail to ask the actual consumer

- need to measure the success of a use case
- government needs to hear the voices of the citizen at the beginning of the regulation making

Fast digital transformation

- are the governments implementing a proprietary way or a standard way

You cannot typically delete your private data from the government. However, there are often provisions for correction and access to the data, depending on the ecosystem.

Next Talk:
Concept of different policies can be automated with standards

- a big identity regulation to standards implementation divide
- Government use them for their purpose
    - different interpretation between two parties
    - Difficult to implement it
- Standard groups try to help with the implementations
- Big hole between interpretation and implementation
    - Audience agrees
- Growing regulations in the identity field, world wide

- Changing paradigm
    - Governments propose technical reference like the ARF
    - Must be implemented and maintained in the end to be compliant
    - Vendor lock-in needs to be addressed because it's very expensive to be compliant with all the regulation and vendor lock-in is undesirable across multiple issue areas.
- Difference between Governance and governance
    - how can we align them for true governance in the trust
    - Most of the audience agrees there is a difference
    - There are many types of governance, and there are now many governance models that have been standardized.
- Harmonization in the different topics like authentication
    - difficult task because a lot needs to be considered
- Trust Framework alignment
    - In the end the product implementations will be attested once
- Narrowing the Gap
    - Identity, Establish, Implement, Attest for minimum viable components
- Enforcement of authentication controls
    - Implementation can be really complex, security can not maintained across the parties
- Next steps
    - Go up the line since it's based on practical examples for a minimum authentication profile
    - Allows inflight attestation
    - Profiles will reduce the gaps between the different solutions

Audience feedback

- good to get internal details to understand the problems
- test driven requirements for the best approach
- proofable trust is as valuable as credentials where the trust is used
- Doing a lot gap analysis
- A lot of discussion is connected to GDPR
    - it's data protection, not privacy protection
- If the understanding of the framework is not clear, how can we implement it in the best way
    - How can we bring the principles like the privacy ones into a system
- interoperability across all use cases will be next to impossible
    - need security aspect for specific things like authentication
    - we can try to reduce the risk to narrow the gap on compliance
- We can talk about it, but we have to do it in practice

2.5. Shared Declaration

This plenary session explored the question of whether or not we should issue a declaration at the conclusion of the Summit.

While the initial survey showed that 72% of respondents supported the idea of a declaration, the ensuing discussion saw support weaken significantly and by the time of the poll, less than 40% of participants agreed that a declaration would be worthwhile to pursue. Ultimately, the term “declaration” may have been the issue, as it connotes a level of legitimacy and weight as well as specific norms within government and multilateral organizational contexts.

Key takeaways:

- We should focus on the outputs of the meeting and or a strategy rather than simply authoring yet another statement of principles. OECD’s recent Recommendation on the Governance of Digital Identity is widely recognized as the most up-to-date and comprehensive statement of principles. The OECD Recommendation provides the kind of substance that might be included in a declaration, it has the benefit of formal due process
- Declarations are difficult and require significant work in advance of a convening. It would be difficult for governments to join as signatories, and some organizations would require a significant lead time to sign on. It would not be possible for more organizations to sign up to a specific declaration, or even to agree to pursue one in the SIDI context.
- Rather than a “declaration” a blueprint or roadmap might be a more appropriate output from this group.
- There was support for SIDI hub next steps and tactics, and future opportunities for in person and online engagement, but a “declaration” is not one of the tactics with broad consensus and support. The SIDI volunteer resources and focus is likely better spent on other tactics in 2024.

Raw Notes

- 72% for a declaration
- Key principles
    - Respondent 1
        - I would like to hear from countries
        - What problems still need solving?
            - Principles for Sustainable Development
            - OECD
            - What are the gaps?
        - Focus output on that rather than replicating other principles (OECD, etc.)

- Respondent 2
  - Report on what we have done here today
  - Bringing the ecosystem together is a big step
  - We still need to define gaps
  - OECD recommendation is just principles
  - Experts here can help add an additional layer
  - Trust framework mapping is still necessary
  - Help OECD help countries
  - Declarations are hard…. Typically a lot of pre-work goes into them. It would be hard to do in this instance.
  - Engaging stakeholders adds credibility…this process was really impactful for the OECD recommendations.
- Respondent 3
  - Yes on declaration
  - The Universal Declaration on Human Rights is always useful in crises.
  - We need to continue to measure ourselves.
  - Measurement is difficult….SDGs are useful.
  - Help sell ourselves to the rest of the world.
  - It should be powerful.
- Floor
  - What is the purpose of the declaration?
    - Vision or operational?
    - Roadmap?
    - What type of declaration?
  - Concern about optics
    - Questions about the institutions represented at the Summit and perceptions about their potential motivations
    - It is hard to communicate what we have done here, which could create new barriers
    - Some would need to get approval to support a declaration
  - Maybe a Blueprint rather than a declaration
    - Considerations
    - Examples
    - Pros/cons
    - Recognize differences between global N and S
  - A declaration could also have downsides
    - Also, I don't like the idea of not telling anyone….transparency is important
    - Anything we put out should emphasize human rights, self-sovereignty, etc.
  - We should…Competitors are coming together to address real-world issues.

        - Not money driven…collaborative.
        - Not prescribing solution
    - Maybe declaration is the wrong word, and another word might make it easier
    - Governments need top-level buy-in to make progress,
        - Often comes from security ministries
        - How do we get it on the PM/President's agenda?
    - Frame as an invitation rather than a declaration.
- Soft (consensus)...but how soft?
    - Getting the UN to sign anything is hard.
    - Who are "we"?
    - What types of organizations?
    - Light governance, but some identity is required.
    - What is the scope of the declaration?
    - Wide or narrow?
        - Interop over the next 10 years?
    - What are the use cases?
    - What are we aligned on trying to do?
    - We need to hear more from governments about cross-border use cases in low-income countries. We need to drill down in a future event with more time for them to express their needs.
- We need to make some statement
    - Interop is important and warrants a statement,
    - Don't only focus on cross-border.
    - Connecting ID programs
- The poll question should now be interpreted as suggesting a "soft declaration"

2.6. Champion “Cross Border” Use Cases

Discussions for Use Cases and interoperability were discussed at length. A main question was to ask what would be the most important use cases?

A definition of the Cross Border discussions, could be *“Cross Border Digital Identity Ecosystem with mutual recognition”*.

Sticky notes were passed around to vote for Digital ID where the attendees were asked to make a distinction between what were defined as EASY Use Cases, compared to HARD But Urgent Use Cases, involving Cross-Border Jurisdictions.

The audience was presented with a 3x3 grid matrix table on screen with row headings of:

- Regulated HIGH Trust
- Regulated BASIC Trust
- Unregulated Use Cases

A question was asked about whether there was a definition for the object (such as Supply Chain) rather than for natural persons.

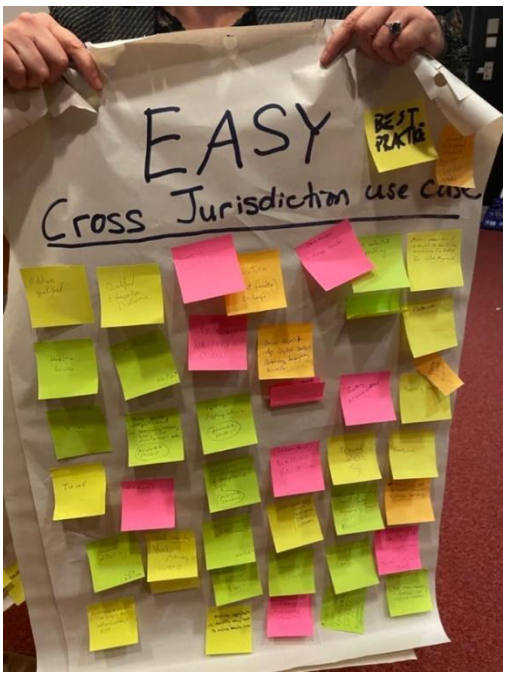
Maritime was used as a key example for roles, rather than being constrained to transactions purely presented as persons.

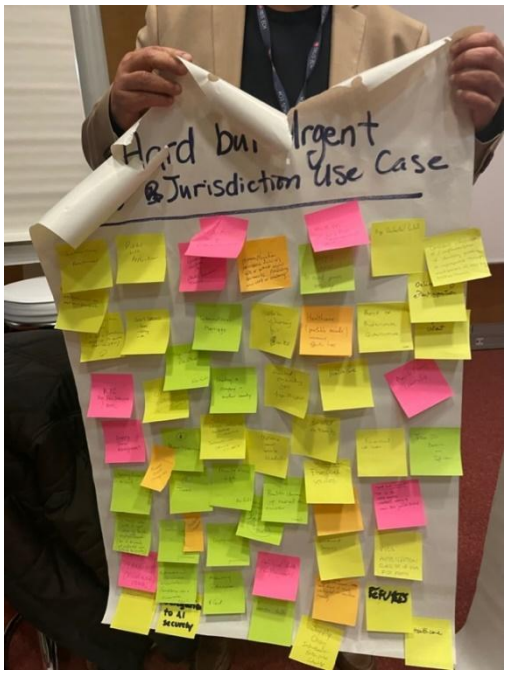
To judge the feel of the room, 2 Whiteboards were provided for members to place their thoughts on what would constitute, in their opinion, **Hard but Urgent**, and **EASY** Use Cases. Each participant was invited to post 2 “champion” use cases for Hard and 2 for Easy. The list of use cases are shown here ordered by the rough number of votes for each. Overall, we see a wide range of use cases, with some repetition across “Easy” and “Hard” where the participants may have had different views or contexts informing why for them it might be perceived to be easy or hard.

“Champion” Use Case Recommendations

"Easy"	“Hard but Urgent”

• Qualifications (10)
  ○ Student & faculty mobility
  ○ Qualified educational degree/ certificates
  ○ Skills qualifications (work or schooling)
• Travel (8)
  ○ Booking portals
  ○ Accommodations
  ○ Plane/ train tickets
  ○ Insurance
  ○ Car Rental, cross border driving
  ○ Passenger screening
• Financial Services (6)
  ○ Mutual recognition of a banks auth mechanism (e.g. FIDO)
  ○ Money transfer
• Government Services (6)
  ○ Citizenship, voting
  ○ License to drive
  ○ Deflect verifications from a central database
  ○ Right to remain (and not work)
  ○ Right to remain and work
  ○ Right to cross border work, small artisanal workers cross border trade
• Access to restricted resources online (3)
• Healthcare (2)
• Supply Chain (2)
• Address qualified (1)
• IoT (1)
• Unregulated, private sector use cases (e.g. LinkedIn, digital platforms) (1)
	• Financial services (11)
	  ○ International Remittances (fiat, crypto)
	  ○ KYC for Financial Services and AML, open accounts
	  ○ Data sharing for banks
	• Qualifications (11) (Education enrollment and degrees, Skills qualifications)
	• Healthcare (impacts lives) (7)
	  ○ Portable records
	  ○ Trusted Onboarding
	  ○ Insurance
	• Government Services (7)
	  ○ Taxes
	  ○ Voting
	  ○ Digital signatures
	  ○ Other
	• Travel (7) (e.g. passports, electronic visa, epassport+evisa, cross border driving)
	• Age verification (6) e.g. adult content in Utah, face to face age
	• Supply chain management (4)
	  ○ Individual
	  ○ Companies (e.g. green washing,food security, CO2 tracing, enterprise identity)
	• Human migration – Re-establish Digital ID with or without documents, for new work or residency (3)
	• Social networking (1)
	• Parent/ child/ caregivers (1)
	• AI delegation Securely (1)
	• Consistent interpretation and implementation of proofing as represented in mechanisms of trustworthiness (1)
	• International Marriage (1)
	• Start a company in another country (1)
	• Foreign worker wants to report abuse, when documents have been taken on entry to country (1)


EASY
Cross Jurisdiction use case


Jurisdiction use Case

2.7. Wrap-Up

The SIDI Summit co-organizers asked the room if they thought the work needed to continue in 2024? Nearly all hands were raised (a fact the Exit Poll also reflects, 92% of attendees agreed).

The SIDI Summit co-organizers thanked all the participants for their attendance, requested that they start submitting their answers to the Exit Poll, and provided directions to the post Summit reception location.

Final instructions for the use case voting was given, so people could add their votes on the way out. The audience was also given an opportunity to vote on “where & when” to meet in person for Summit(s) in 2024. These venues/ events were proposed by the audience.

- Japan
- ID4Africa
- Mobile World Congress
- IETF Brisbane
- IETF Canada
- Mosip Connect (March)
- Barcelona or Miami (to get Latam involved)
- Trustech
- Nigeria – week of identity

In closing, the audience gave a round of applause to the organizers.

Appendix 1: Pre-Reading for the SIDI Paris Summit, 11/28/23.

Published at: https://sidi-hub.community/reading-list/

Strategy Session

"Model Governance Framework for Digital Legal Identity." UNDP, September 2023. https://www.governance4id.org/
Garber, E. and Haine, M. (eds) "Human-Centric Digital Identity: for Government Officials," OpenID Foundation, September 2023. https://openid.net/Human-Centric-Digital-Identity-Final
lanagan, Heather, ed. "Government-Issued Digital Credentials and the Privacy Landscape, v1.1." OpenID Foundation, August 2023. https://openid.net/Government-issued-Digital-Credentials-and-the-Privacy-Landscape-Final-v1.1.
"OECD Recommendation on the Governance of Digital Identity." OECD, June 2023. https://www.oecd.org/digital/digital-government/oecd-recommendation-on-the-governance-of-digital-identity.htm
"Digital Identity Roadmap Guide." ITU-T, 2018. https://www.itu.int/en/ITU-D/ICT-Applications/Pages/digital-identity.aspx
"Giving Voice to Digital Identities Worldwide" Secure Identity Alliance, February 2021. https://secureidentityalliance.org/digital-id-sia-publications/giving-voice-to-digital-identities-worldwide-1-1
"Guidance on Digital /iD.", Financial Action Task Force, March 2020. https://www.fatf-gafi.org/en/publications/Financialinclusionandnpoissues/Digital-identity-guidance.html
"On the Road to User-Centricity: Digital Identity in the Electronic Wallet Era", Secure Identity Alliance, November 2022. https://secureidentityalliance.org/utilities/news-en/on-the-road-to-user-centricity-digital-identity-in-the-electronic-wallet-era-1

Technology Session

"DIACC Briefing: Introduction to Identity Interoperability," DIACC, April 2023. https://diacc.ca/wp-content/uploads/2023/04/DIACC-Briefing-Introduction-to-Identity-Interoperability.pdf
"Why the World Needs an Open Source Digital Wallet Right Now.", OWF. https://www.linuxfoundation.org/research/open-wallet-foundation
Alamillo, I., Stefane Mouille, Andrea Röck, Nicolaos Soumelidis, Michal Tabor. "Digital Identity Standards." *ENISA*. July 2023. https://www.enisa.europa.eu/publications/digital-identity-standards

Trust Framework Analysis and Alignment Session

"DRAFT EU-US TTC Digital Identity Mapping Exercise Report", US-EU Trade and Technology Council Working Group 1: Technology Standards Subgroup on Digital Identity, December 2022. https://www.nist.gov/system/files/documents/2023/12/22/EU-US%20TTC%20WG1_Digital_Identity_Mapping_Report_Final%20Draft%20for%20Comment_22122023.pdf
"A Guide to Trust Frameworks for Smart Digital ID", OIX. https://openidentityexchange.org/a-guide-to-trust-frameworks-for-smart-digital-id?page=overview
"Pan-Canadian Trust Framework", DIACC. https://diacc.ca/trust-framework/
"Digital ID DNA – Interoperability Across Trust Frameworks.", OIX, October 2023. https://openidentityexchange.org/networks/87/item.html?id=708
Garber, Elizabeth, Nick Mothershaw, Stephanie Labriolle, Debora Comparin. "GAIN in 2023." July 2023. https://openid.net/announcing-gain-in-2023-whitepaper/