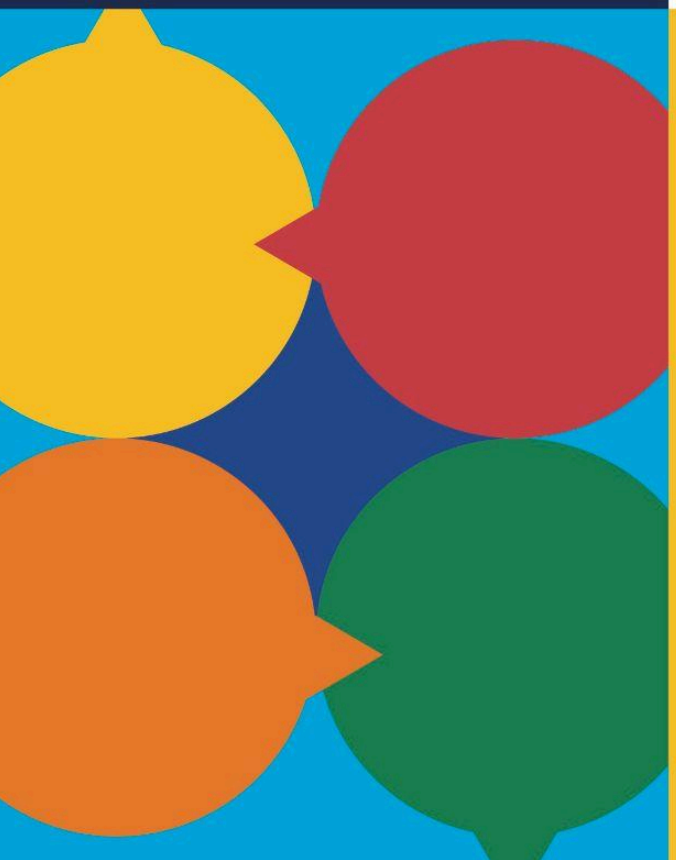
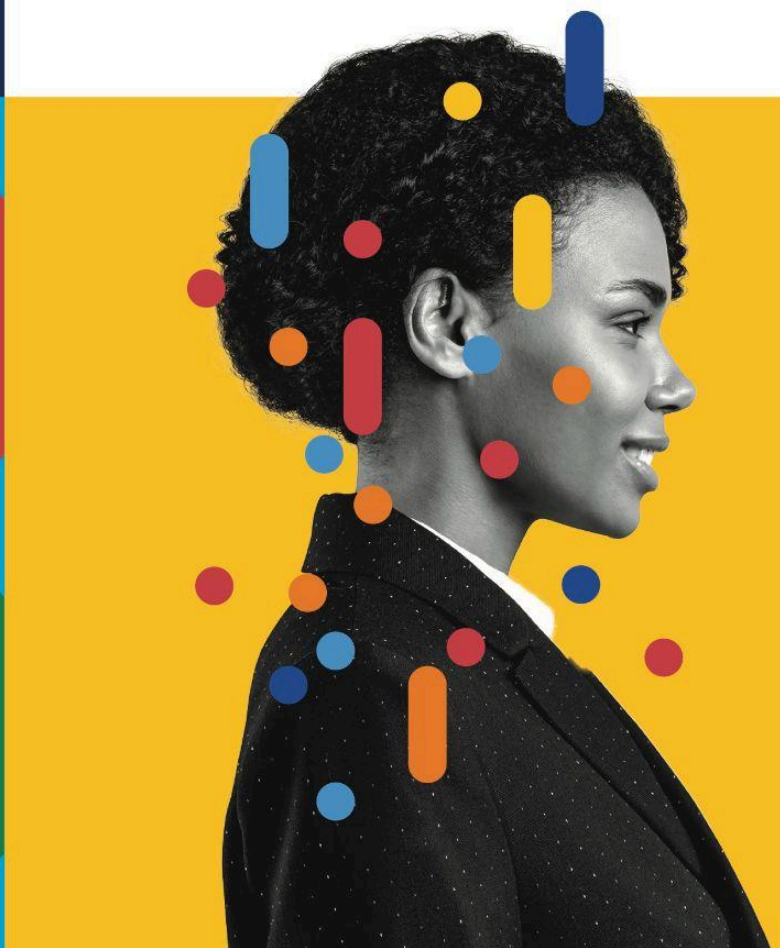
MOSIP connect 2025

unConference

Book of Proceedings

Exploring MOSIP-led Digital Transformation





Contents

Executive Summary

Why MOSIP unConference?

In 2024, we had the first ever MOSIP Connect in **Addis Ababa, Ethiopia**, where we convened over 400 participants from stakeholder and partner organizations and the digital identity community. While we were excited at the growth of the MOSIP ecosystem, we started to feel the challenge of hearing the voices of the community and unlocking its collaborative potential. As a result, we decided to introduce unConference to the second day of MOSIP Connect in 2025, enabling the community to freely propose and discuss topics of interest after a day of MOSIP updates and curated topics by our team.

"The unConference created the perfect space for a very meaningful set of conversations. We could not have prepared a better agenda. We hope to use these learnings to inform MOSIP's work and improve our conversations in the future."

– Ramesh Narayanan
Chief Technology Officer, MOSIP

How It Worked

The **MOSIP unConference** followed an **Open Space Technology** format, intentionally designed to foster engaging conversations and action-oriented collaboration rather than traditional passive listening. In contrast to the first day where most participants were in listening mode. There were no keynotes or fixed panels; instead, the event focused on dynamic, participant-driven engagement.

The day began with a **collective gathering**, where participants gathered at 8:30 AM to propose and prioritize topics of interest and co-created the agenda for the day by selecting a session space and time for their proposed topic(s). The attendees co-created the agenda for the day. The group then self-organized into smaller sessions based on the agenda that included interactive discussions, hands-on workshops, spontaneous panels, and informal networking, across five **focused working sessions**.

Notetaking is important because sessions take place in parallel. We provided the tool of QiqoChat and guidance for participants to take and share notes. Notes could be taken by participants who volunteered to do so during sessions or added by the hosts post sessions. Depending on the notetakers' capacity and familiarity with the topics, the quality and accuracy could vary. All available notes have been compiled in the "Book of Proceedings".

Advantages

Unlike conferences with agendas pre-defined by organizers, a good unConference puts in place the right structure to unlock, on the day of the event, participants' generative

energy to become session hosts and co-create content with fellow participants. The combination of the conference and unconference formats worked very well in our case, as the first day of keynotes and panels set the MOSIP ecosystem context for a productive participants-led co-creation on the second day.

We found the following particularly true about the MOSIP unConference:

1. **Empowered Participants**: Created strong momentum for participants Empowered attendees to shape the agenda based on real-time interests and priorities, with many proposing multiple topics.
2. **Highly Collaborative**: Encouraged open dialogue and active contribution from all participants.
3. **Action-Oriented**: Focused on problem-solving and knowledge exchange rather than passive presentations.
4. **Flexible & Adaptive**: Created space for emerging ideas, spontaneous collaboration, and deep exploration of relevant topics.
5. **Inclusive Engagement**: Leveled the playing field, where everyone had the opportunity to propose and lead sessions, regardless of title or affiliation.
6. **Cross-Pollination of Ideas**: Brought together diverse perspectives across geographies and sectors, fostering innovation and co-creation.

Key Topics Discussed

There were 16 primary spaces and five session slots altogether, which provided capacity for 80 sessions. We ended up having 57 sessions and over 250 participants engaged on the unconference day, covering the following main areas of topics:

1. **Verifiable Credentials & Trust Models**
    - Emphasis on scaling issuers and verifiers using privacy-preserving protocols like Zero Knowledge Proofs (Reclaim Protocol).
    - Growing interest in converting national IDs into verifiable credentials, with standardization via OpenID4VC.
    - Challenge remains in unifying and simplifying credential formats across diverse ecosystems.
2. **Fraud Prevention in Biometrics**
    - Key biometric fraud issues: fake fingers, spoofing, swapped hands, and data manipulation.
    - Solutions include better operator training, liveness checks, quality analysis, and software validation for anomalies.
3. **Refugee & Inclusion Strategies**
    - Designated organizations and countries are integrating refugees into national ID systems using MOSIP and biometric interoperability.
    - Emphasis on balancing inclusion with data protection and verification.
4. **Rural & Farmer Enrollment**
    - Strategies to boost rural registration included incentive-driven campaigns, door-to-door outreach, and linking benefits like subsidies to digital ID.
5. **DPG Deployment**
    - Need for scalable strategies, localized support, and integration of DPGs like OpenCRVS and MOSIP.

- Countries are seeking guidance on procurement, customization, and community engagement for effective rollout.
- Provide the most fundamental DPGs in a box

6. **Brownfield Implementation & Data Migration**
    - Migration from legacy ID systems to MOSIP is complex, involving data quality, deduplication, and workflow customization.
    - A clear roadmap and country-specific support are essential.
7. **Digital Identity Without Biometrics**
    - Explored approaches for issuing IDs through alternate mechanisms instead of storing biometrics, using public-private key pairs and face recognition.
    - Consider registrations without biometrics, in case of countries with smaller populations.
8. **Private Sector & DPI Adoption**
    - Key to success: enabling policies, trust-building, flexible regulation, and promoting innovation.
9. **Instant ID Issuance**
    - While vendors propose instant issuance, concerns around deduplication and verification remain an area of concern.
    - Various approaches were discussed.
10. **Impact & Accountability**
    - Discussion around how to define, measure, and communicate impact of digital ID systems.
    - Emphasis on centering end-users and acknowledging both successes and failures.

In **summary**, the MOSIP unConference 2025 showcased the power of open, collaborative dialogue in driving real progress. With no pre-fixed agenda, participants shaped the discussions, resulting in focused, action-oriented sessions on key topics like verifiable credentials, biometric systems, and inclusive digital ID strategies. The format fostered genuine knowledge sharing, peer learning, and cross-sector collaboration.

As we move forward, the lessons, connections, and collaborations sparked during this event will continue to guide and inspire our shared mission of building inclusive, secure, and interoperable digital ID systems.

We thank all participants for their contributions and look forward to their continued engagement in the journey ahead.

Disclaimer

The session notes (“Notes”) collected and compiled by the MOSIP team on the following pages are intended solely as a summary of discussions and ideas shared during the MOSIP Connect unConference 2025. MOSIP disclaims all responsibility for the accuracy, completeness, or verifiability of the content presented in the Notes. The Notes reflect the perspectives and contributions of participants and does not represent official positions, endorsements, or commitments by MOSIP.

Notes may be contributed by session hosts or attendees. Any claims, statements, or conclusions made in the Notes are not attributable to MOSIP or the hosts/facilitators, nor are they verified by them. As the Notes are based on open discussions and participant-driven dialogue, they should not be relied upon as definitive or authoritative.

MOSIP shall not be held liable for any errors, omissions, or interpretations arising from the use of the Notes. Readers are encouraged to independently verify any information contained herein before relying on it for decision-making or other purposes.

By accessing the Notes, readers acknowledge that MOSIP disclaims all warranties and liabilities related to its content.

For information on how MOSIP handles intellectual property, please refer to our IP Policy.

Session 1

Room B

Challenges of Onboarding and Scaling Issuers of Verifiable Credentials

Session Convener: Subhash/Kartik (Reclaim)
Session Attendees: 10-13 attendees

Specific Country / Technology Discussed: Zero knowledge proof / https verifier

Tags / Themes of the session:
VCs beyond identity — tamper evident
Reclaim use cases

Links to Resources:
https://reclaimprotocol.org/

Notes

- Current challenge of doing manual background verifications (Eg: employment or student verification) where the institution issuing certificates are approached.
- Distributed issuers should be addressed to trust the data. Verifiers should also trust the issuer.
- To integrate to VC , scaling issuers is difficult due to legacy issues, considered not a priority, lack of content/ clarity/ motivation, technology limitations, not a primary responsibility, identify real need, each department of govts to be streamlined
- Reclaim acts as a digital notary system by attesting the user data and sending it to the relying party trying to ensure user authentication.
- Reclaim is a zero-knowledge proof, https verifier. Currently supporting UCs where the user is aware of the credentials to access a specific website from where data .
- Login to website --> data proof generated --> store data in relying party portal
- Reclaim only receives encrypted data . (UCs applicable- Student verification through university portal, HRM portal, Job Marketplace). Cryptographically signed data transfer.
- Advantages compared to biometric systems: No hardware/ integration cost. Catch is user needs smart phones , govts need not integrate with multiple systems- as user data is already present in existing portals, selective data revelation

Unanswered Questions
Is there a need for a centralised database?

Next Steps / Action Items:
Govts to support adoption and then on field challenges can be addressed in real time as the product is evolving.

Room D

Best Practices for One Source of ID Systems

Session Convener: Andrea (Philippines)

Specific Country / Technology Discussed: Philippines

Notes

- Identifying the other countries — what different ID systems do they have?
- Mapping bank accounts linked to the national ID
- Incentives for social benefit transfer.

Room F

Navigating DPG-Country Relationships
Strategies for Effective Collaborations

Session Convener: Swarathmika (MOSIP)

Notes

Key Points on DPG Engagement Principles:

- Many DPGs operate with non-binding MOUs that establish principles while limiting liability
- Flexibility is necessary but must balance with core principles
- Civil registration systems often have limited funding, requiring adaptable approaches

Main Concerns for DPGs:

1. Data Protection & Liability
    - Most DPGs emphasize "we don't touch production data" as a core principle
    - When exceptions are necessary, they require formal agreements with liability clauses
    - Many DPGs avoid direct data access entirely: "We don't touch it. We don't want it."

2. Implementation Models
    - Evolution from direct implementation to advisory roles
    - Growing emphasis on building local capacity and ecosystem of System Integrators (SIs)
    - Challenge of balancing standardization with country-specific customization

3. Open-Source Contributions
    - Strong desire for countries to contribute customizations back to the core codebase
    - Helps prevent countries from "forking" and losing access to updates
    - Creating shared value through code contributions, experience sharing, and promoting DPGs

Country Engagement Considerations:

4. Ethical Dilemmas
    - Working with countries lacking data protection laws or with surveillance concerns
    - Question of whether DPGs should refuse engagement or try to influence from within
    - Different approaches: some DPGs reject certain engagements; others believe providing good systems is better than alternatives

5. Technical Understanding

    - Countries often have limited understanding of open-source benefits
    - Need for education about long-term advantages of staying with core platform
    - Challenges explaining security benefits of open source versus proprietary solutions

6. Legal & Regulatory Frameworks
    - Most constraints are country-specific regulatory requirements
    - Some DPGs report their biggest constraints come from their home country regulations
    - Positive trend of some countries adopting data protection laws after implementing DPGs

Wish List for Country Engagement

<u>From DPGs to Countries:</u>

- Contribute code modifications back to the community
- Share experiences and learnings with other implementing countries
- Participate in co-development of new features
- Help spread awareness about DPG benefits

<u>From Countries to DPGs:</u>

- Assurances that engagement won't jeopardize government data
- Better understanding of open-source security benefits
- Recognition of DPGs' ongoing support (unlike traditional open-source projects).

Room G

Technologies to Reduce/Eliminate Fraud During Biometrics Enrolment

Session Convener: Nanyanzi Grace

Session Attendees:
- Hedwig Orieba & Shahid, Mantra technologies, Uganda
- Sam Jefferies, UNHCR
- Dr. Ted Dunstone, BixeLab (biometric testing)
- Abel, National ID Program, Ethiopia

Specific Country / Technology Discussed: Uganda, Ethiopia

Tags / Themes of the session:
Biometrics
Fraud
ABIS

Links to Resources:
https://www.gov.za/services/verify-identity-online (banks have adopted this)

Notes

- Mass enrollment: mobile enrollment kits, identify the office
- Modalities: face & 10 fingerprint collection (base minimum quality requirement)
- Before card printing the biometric modalities are de-duplicated
- Network connectivity is a challenge, but a hybrid collection of data

Frauds/Challenges:
- Swapping of left & right hands
- Using toe fingers
- Mixing of fingerprints
- Lack of background checks on the operators (they don't cheat in the beginning, but when the trust is built)
- People with amputated/bandaged hands
- People clicking picture of iris scan images upside down
- old face pictures, their face/posture also changes over a 10-year
- Face SDK: has an override option, large scale of operation with timelines
- Operator's KPI is number of registrations/enrollments
- Fake fingers, people taking a picture of a person, fake fingers have defects in them
- Camera injection attacks are possible
- OTPs in India are often misused to 'mis-represent' people
- Fraudulent use of dead people's identity
- Liveness proof
- Ghost-workers still getting pensions

Fraud Management Solutions:
- Instantaneously detect mismatch of finger, swapped hand, use of toes

- use of police
- Review & analysis of the quality profile of the fingerprints collected by the agents to cut out unacceptable shortcuts
- Enroll the operators first into the biometric system so that they don't re-register themselves
- An amputated person can't add a finger later, but an ex-bandaged person can
- Hardware limitations preventing an upside-down iris, software detection for upside down iris
- Enhance signatures/images^(remove backgrounds, shadows) but not the biometrics
- Identity resolution factors: biometrics, face, geographic profile
- Manual overrides to accept facial data can be quarantined before being written to the back-end
- Operator's KPIs: can also be incentivised for biometric capture quality; while having safety checks so that the older population with lower quality biometrics aren't not marginalised
- Ethiopia has audits & data verification being done by fewer employees but it increases the time-to-enrollment
- Taking statistical samples of data and look for trends and check & flag the frauds by various factors such as the enrollment center, operator, location
- Liveness check is now common by bio-SDK, passive liveness checks can also be done, prompting the person to blink/nod so that generative ai
- Camera injection attacks: avoid using web browser or mobile apps
- Fraudulent use of dead people's identity: registering death, same number is not re-registration
- Liveness proof: a liveness check via an app to get pension, can alternately go to the bank to prove that the person is alive.

Unanswered Questions

These can be questions raised during the session that did not find a conclusion, were unaddressed, or deserve further discussion!

- How to beat deep-fakes?
- Check for camera injection attacks?

Next Steps / Action Items:

Hiring operators with high integrity should solve most problems, most frauds are internal.

Room K

Strategies to Increase Registrations in Rural Settings

(Combined Session)
Key actions for mass registration& integration for successful digitization / ID registration in rural setting / How to navigate different use cases for national ID enrolment

Session Convener: Ephem M

Specific Country / Technology Discussed:
Ethiopia

Tags / Themes of the session:
How to increase registrations?

Notes

The meeting focused on strategies to encourage farmers to register in the national ID system. The objective was to gather insights from various countries and experts on effective approaches to increase registration rates. A key priority for governments is to ensure widespread farmer enrollment to facilitate the distribution of agricultural aid and strengthen the agriculture sector.

Key Discussion Points & Recommendations:

1. Integrated Agricultural Platform:
- Develop a centralized system integrating inputs, fertilizers, credit, insurance, and market linkages.
- Simplify access and reduce costs by consolidating services into a single platform.

2. Tailored Digital ID Enrollment Strategies:
- Assess reasons for both registration and non-registration among farmers.
- Analyze demographic and societal factors influencing adoption.
- Leverage data-driven insights to improve outreach and engagement

3. Increasing Enrollment Through Government Engagement:
- Learn from best practices in other countries.
- Identify and address barriers to farmer registration.
- Strengthen government initiatives linking agricultural benefits (e.g., loans, subsidies) to digital ID enrollment.

4. Government Incentives & Citizen Adoption:
- Introduce financial incentives such as subsidies and assistance programs to encourage registration.
- Implement a bottom-up approach, ensuring farmers experience tangible benefits.
- Foster collaboration between government, industry, and financial institutions to enhance farmer support.

5. Technological Considerations for Registration:

- Explore innovative and accessible registration technologies.
- Address challenges such as high resource requirements and accessibility in remote areas.
- Implement door-to-door registration strategies to reach rural populations effectively.
- Adapt approaches to accommodate large rural populations (approximately 70-85% of total).

6. National Agricultural ID System:

- Evaluate the current status and challenges of a unified farmer ID system.
- Enhance data collection efforts and ensure seamless integration with the national ID system.
- Prioritize accuracy, accessibility, and inclusivity in the registration process.

Conclusion:

The meeting emphasized the need for a multi-faceted approach, combining government policies, incentives, technology, and tailored outreach strategies to maximize farmer participation in the national ID system. Collaborative efforts across sectors will be essential to achieving widespread adoption and ensuring that farmers benefit from digital identification.

Next Steps / Action Items:

- Farmers without proper identification facing barriers.
- Software and data inconsistencies impacting registration efforts.
- Strategies for improving outreach and engagement in rural areas.

Room L

How can we make it easy, cheap, and fast to deploy DPGs at scale?

Session Convener: Ed Duffus, OpenCRVS

Tags / Themes of the session:
How to find the right DPG for a country?
How to tackle economic capabilities?
How to create a DPG model?
Overview of Upcoming Initiatives and Challenges

Notes

DPG Stack is dependent on:

- Infrastructure: Data centre setup
- Software Module : S/w module required for the realization of the DPG.
- Government Policies : Legal framework, government policies , institution that would be involved in decision making of the policies involved for DPG.
- Funding: Main factor for the project to be implemented and maintained.

Countries Involved:
- Somalia
- Burkina Faso
- Madagascar
- The Philippines
- Uganda

Potential for six countries in total within a few months.

Current Strategies:
- Reference implementations are being utilized.
- Discussion on the role of DPG (Development Partnership Group) in implementation.

Challenges Identified:
- Lack of scale in country development.
- Integration issues within the ecosystem.
- Need for more effective deployment strategies.

Future Prospects:
- Strong sales pipeline for OpenCRVS with 20-25 countries showing engagement.
- Potential for similar demand in countries of comparable size and development stage.

Important Details

- The DPG is involved in implementation but is not sufficient for achieving desired scale.
- There is a recognition of the limits of current country development efforts.
- The discussion suggests a need for broader strategies beyond just OpenCRVS.

Key Information

- The meeting included a brief intermission, with participants expressing gratitude and confirming note-taking responsibilities.
- The conversation indicates a proactive approach to addressing developmental challenges in multiple countries.

Conclusion
The discussion highlights the ongoing efforts and challenges faced by the DPG in implementing development strategies across several countries. While there is a promising pipeline for future engagement, significant barriers related to scale and integration remain. The need for innovative strategies to enhance country development is emphasized, pointing towards a collaborative approach in addressing these challenges.

Room O

Challenges with Multiple Duplicate Registrations in PSA

Session Convener: Philippine Statistics Authority (PSA)

Notes

The session focused on addressing cases where individuals re-register for a national ID, often in good faith, believing they have not received their physical ID. The discussion explored potential technology-driven solutions for PSA to manage and mitigate such instances effectively.

Objectives

- Share experiences from national ID registration processes.
- Identify solutions to reduce multiple registrations in PSA's National ID system.

Identified Use Case: Individuals revisit registration centers to register again, assuming they have not received their physical ID.

Key Questions Raised:

- Does PSA register individuals offline, or is registration primarily online?
- How is the verification of registrants conducted, demographically or biometrically?
- Are multiple registrations a case of fraud or genuine misunderstanding?
    - *Thales authentication:* If the issue is fraud prevention, deduplication is the only solution?
- Can authentication methods, such as Wise Authentication, help eliminate ghost recipients (e.g., fraudulent pension claims)?
- Can we carry out verification at the time of registration itself?

Current PSA Measures:

1. Existing Systems: FindMyTRN and WIMNID (Where is My National ID?) help track registration status.
2. Public Awareness Initiatives: PSA has made significant efforts to inform the public about avoiding duplicate registrations, as these contribute to backend processing delays and prolong ID issuance.

Conclusion:
Addressing multiple registrations requires both technical solutions (such as biometric deduplication and authentication mechanisms) and improvements in business processes (such as enhanced public awareness and registration tracking systems).

Next Steps / Action Items

- **Reduce Backlogs:** Prioritize clearing existing registration backlogs.
- **Strengthen Public Awareness:** Educate registrants on the registration process to prevent duplicate entries.
- **Technical Exploration:** MOSIP will internally discuss with the development team to explore possible solutions to mitigate this issue.

Room T

Digital Identity and Verifiable Credentials

(Spanish with consecutive interpreting)

Session Convener: Cesar Rosales Maquera

Specific Country / Technology Discussed:
Peru, Verifiable credential, Inji, ID Peru

Tags / Themes of the session:
Issues and constraints, Verifiable Credentials

Notes

Overview
This session focused on global experiences with digital ID systems, discussing security, adoption, and regulatory aspects. The discussion included examples from India, Peru, and Bolivia, examining both technical and cultural challenges of migrating from physical IDs to digital credentials.

Key Discussion Points

1. **Security and Testing**

- Emphasis on comprehensive security testing (both defensive and offensive approaches).
- Importance of adhering to best practices for digital identity security.
- Necessity of setting up robust monitoring and security apparatus to detect and respond to threats.

2. **Chip-Based vs. Chipless Cards**

- Countries experimenting with various formats for identity cards:
- Bolivia: Introduced cards with a printed fingerprint image, but encountered usability and aesthetic concerns.
- Peru: Transitioned from printing large fingerprints on cards to smaller ones, with legal requirements for fingerprint display still in place.
- Discussion on whether chip-based cards provide stronger security, and how visual features (like fingerprints) can influence public perception and acceptance.

3. **Transition from Physical to Digital IDs**

- India: Encouraging the public not to carry physical IDs.
- Promoting digital ID usage with biometric verification.
- Goal is to enable multiple use cases and widespread adoption of e-cards.
- Peru:
    - Introduced chip cards for first-time registrants but still uses non-chip plastic cards widely.
    - Resistance often stems from fear of change, misinformation, or cultural attachment to physical documents.

4. **Regulatory and Cultural Challenges**

- Many countries have regulations dating back decades, complicating the shift to digital identity.
- A key challenge is ensuring existing frameworks align with new digital systems.
- Cultural acceptance and trust in digital credentials remain major hurdles.
- Need for political willingness and clear policies to guide the transition.
- Strategies for Adoption
- Education & Outreach: Public awareness campaigns to explain benefits and security features of digital IDs.
- Incremental Rollouts: Gradual expansion of use cases to build familiarity and trust.
- Stakeholder Engagement: Collaboration between government agencies, private sector, and citizens to address concerns.

Action Items & Recommendations
Documentation of MOSIP in Spanish can help with adoption in Spanish-speaking countries.

Conclusion
The session underscored that moving from physical to digital identity systems involves not just technical upgrades, but also significant cultural, regulatory, and political considerations. By focusing on robust security, clear policies, and proactive engagement, governments and organizations can foster trust and drive successful adoption of verifiable credentials.

Room W

Designing for Smoother DPI Rollouts — Learnings from the Ground

Session Convener: Vinod

Notes

- When is the right time to generate digital identity?
- In Sri Lanka, you get a national ID after you turn 18.
- Gambia has similar things. CRVS and national ID
- Birth at CRVS, at 18, you have a national ID.
- National ID by Dept of Immigration
- CRVS, world bank, national health insurance authority
- Who generates the ID numbers?

Defining the Need: What problems does ID solve?

- Including Policy Decisions And Clarity On National ID Vs Other Ids.
- Governance And Institutions
- When Can One Get A National ID Generated?
- Who Gets It? Citizens, Residents
- At What Age?
- Different Models
- India (Aadhaar) Model
    - Sectoral IDs Are Linked To Aadhaar Id... Works Ok For Indi, As Central Agency Issues The Id
    - There Are Other Federated Models
    - Align Different Depts
- European Model Of Federates Models
    - Wallet Has Multiple Providers
    - Each Person Holds His ID In His Wallet
- Country Has Multiple Needs
- Civil Registration, Foundational Id
- What If The Beneficiary System Is Rolled Out First, Before Foundational Id.
- Ideally Beneficiary ID Should Be Linked To The New Foundational Id
- Misunderstanding Of CRVS And Id
- Registration Of Birth Is Not Id

Defining the Solution

- MOSIP is a DPG that can be used
- Singapore, India - have their own proprietary solution
- How do you create the RFP?
- guidelines for solution on DPG or irrespective
- local support and expertise
- World Bank projects have to go through procurement... this is an important
- technology and vendor neutral
- foster innovation in local communities

RFP

- Clearly specify your current systems and DPGs that you'd like to integrate with?
- leverage open source, though it not need using DPG
- Do funders fund for that solution (e.g. Foundation IDs)? Or do you fund for more?
- conversation with Govt of the country
- World Bank funds
    - some support with implementation
    - define the tech specs with Govt for the RFP
    - define the IT principles
- Strategy and Implementing decisions are made by the Country
- Evaluations of proposals
- design for inclusion

> What are the best practices to get these DPI solutions?

- Adapt open source

---whatever should be built be built as open-source.

> barrier of inclusion

-design system such that it reaches to the end user where getting basic needs are also difficult.

What are the challenges?

Roll out -> Execution

- Campaign and educate people to get them to get National IDs OR,
    - like Aadhaar make things easier if you have National ID
- Process Change
- Support for local
- Sensitisation
    - some pockets of society may feel this is not for them
- Information and data sharing amongst different govt depts
- Quality of data that can be shared
- Challenges with network connectivity are uncovered during rollouts. Was this tested earlier?

Challenges Faced During Rollouts

- training and change management, process changes, dedicated support.
- interdepartmental conflicts.
- information sharing , quality of data, quality of infrastructure, quality of appliance
- politics related to governance
- where it is getting tested.

Scale Solution and Adoption

- awareness
- some section of people may feel this is not for them, especially people who feel neglected by the Govt
- Well thought off engagement
- Do you make it mandatory for citizens to have National Ids?
- Work with communities and civil societies to have a feedback loop.
- Understand genuine concerns, create a message

Operation and maintenance

- - needs to be well thought out from the start

Session 2

Room B

Why Not Instant ID Issuance?

Session Convener: Antony Vendhan

Session Attendees:

- Thibaut , Famoco
- Hendrik wiermer, OVD kingdom
- Suraj, MOSIP
- Richard Tan, Seventh Sense AI

Specific Country / Technology Discussed:

Africa
USSD - use local de-duplication

Notes

1. Find a way to issue ID instantly
2. Give ID immediately (not acknowledgement number)
3. Perform local de-duplication
4. Issuance based on BIOMERTICS instead
5. Create own instant IDs using existing IDs

Observation: Only vendors attended, no country delegates attended, so it is not an issue for them.

Unanswered Questions:

- ID can't be used until de-duplication is done.
- Can we do de-duplication without internet connectivity?
- Temporary ID can't be used even issued immediately because de-duplication check is not done.

Next Steps / Action Items: Continue to explore different ideas

Room D

Migrating Legacy National ID Systems to MOSIP Platform

Session Convener: Ram Thapa / Ramesh Narayanan

Specific Country / Technology Discussed:
Real-time examples of on field implementations in adopted countries

Notes

- Greenfield/ brownfield implementations and the steps involved.
- importance of studying and analysing existing data structure that comprises demographic, biometric data and the documents that are to be migrated. Checks on integrity and completeness of the demographic data, integrity, quality and completeness of the biometric data are verified
- Challenges such as a) records with missing data such as phone numbers, email IDs, face photo etc, address, b) Records that contain poor quality biometrics, c) Duplicate records may pose a challenge during migration and steps to be taken accordingly
- Creating an inference engine out of the above data can result in decision making such as how many people might have to be called for ID data update., how many ID records have expired, locked or disabled, how many records have no address details in them, no phone numbers and no other contact details, how do we identify such people for renewals, so and so forth.
- Also a thorough investigation about the complexity, performance, endurance and maintainability of the current system has been considered.
- The speciality of MOSIP being modular is that it allows user countries to build custom workflows.

Room H

Digital Identity Without Biometrics

Session Convener: Priyan

Specific Country / Technology Discussed: Tongo ID solution was discussed which is being carried out currently to generate the ID without capturing the biometrics and technology discussed on Cryptographic concept encryption and decryption using public and private keys.

Notes

How can one issue an ID without capturing biometrics?

- If the National ID system is not permitted to capture and store biometrics, obtain support from an organization authorized to store biometrics. Use documentation from that organization to verify the resident manually and issue an ID.
- CRVS system is used to generate a unique number for birth certificate for an individual so this birth certificate is a unique number and the document can be used to verify the person's identity proving that he is a right person and then register with the National ID system to issue an ID.

How can one issue an ID without storing any biometric data?

- If the country cannot store biometrics, scan biometrics (e.g., face) generate a public key against the face, convert it into a template. During verification any government services scan the person's face then a private key will be generated against the face. If the private key's random values match the previously generated public key for the person's face, verification is successful.
- Issue an ID with a QR code containing only personal information such as name, DOB, and gender, excluding biometrics. To verify an individual, scan their face then a private key will be generated against the face which will help to verify the individual's identity by matching the private key with the public key generated during registration.

Room K

OpenID4VC 101

Session Convener: Joseph Heenan

Specific Country / Technology Discussed:
OpenID Connect, VC issuance and presentation

Tags / Themes of the session:
OpenID4VC & OpenID4VP

Links to Resources:
Presentation slides:
https://docs.google.com/presentation/d/1h5FIiM09TNhRk21gPVIVt8pDLO6-KKve/edit?usp=sharing&ouid=107381980093922120275&rtpof=true&sd=true

Notes

Key Components of OpenID4VC - OpenID4VC consists of three main components:

- **Issuer** – Issues verifiable credentials (VCs).
- **Wallet** – Stores and manages credentials.
- **Verifier** – Validates credentials.Discussion PointsNational ID to Verifiable Credentials

A key question raised: Should national IDs be converted into verifiable credentials? If so, how?

- The OpenID Foundation plays a role in standardizing VC issuance and presentation, enabling wallets to convert national IDs into VCs for practical use.

Timeline for OpenID4VC and OpenID4VP
The final **version 1.0** of OpenID4VC and OpenID4VP is planned for release by **June 2025**.
Subsequent updates:

- **Version 1.1** will introduce VC support for multiple encryption mechanisms.

HAIP (Higher Availability Internet Protocol)

- The first version is yet to be released.

Identified Problems and Solutions through OpenID Protocols Credential Format Ambiguity

- No clear definition of credential formats was provided.
- The OpenID specification offers a credential format-agnostic protocol.

Lack of Standardization for Digital Wallets

- No established standards existed for digital wallets.
- The OpenID Connect specification, similar to OAuth 2.0, addresses this gap.

Reluctance to Use Decentralized Identifiers (DIDs)

- OpenID specifications do not mandate DIDs, ensuring a key-agnostic approach.

Trust Without DIDs

- A key concern: How can trust be established without using DIDs?
- In the **EU use case**, trust is maintained through encryption keys held by both the relying party and the issuer.
- The issuer's **root certificate** acts as a trusted entity.
- **PKI (Public Key Infrastructure)** generates various key types, making a centralized key for cross-country authentication impractical.

Global Adoption of OpenID Connect Standards

- Adoption was discussed across various organizations, including:
  - European Digital Identity Wallet
  - NIST (National Institute of Standards and Technology)
  - Japanese Government

Interoperability & Open-Source Contributions

- Key open-source libraries were highlighted.
- Major interoperability events:
  - LSP Potential
  - NIST events
  - ISO/IEC SC17 WG10 interoperability events (mDL)

Security Analysis in OpenID4VC

- Discussion on **attacker models** to enhance security.
- The OpenID4VP recommended draft (24) focuses on:
  - Privacy protection
  - Support for multiple security levels
  - Ease of use
  - Multi-credential inclusion in a single response

Use Cases for Multi-Credential Sharing

- Example scenarios:
  - **Opening a bank account** – Sharing proof of identity and address.
  - **Payment transactions** – Sharing debit card details along with a Starbucks priority card.
- Ongoing research aims to improve seamless multi-credential verification.

Device-Based Presentations

- Discussion on single-device vs. cross-device presentations. Advancements in OpenID4VP
- Development of a new **Digital Credential Query Language (DCQL)** based on community feedback.
- Explanation of data transactions.

SD-JWT for Verifiable Credentials

- Discussion on **SD-JWT VC-SM format** for VC issuance.
- Why SD-JWT?
  - JSON-LD is complex, and SD-JWT was introduced to simplify VC issuance.
  - Supports **W3C VCDM** on top of SD-JWT, enabling transitions between JSON and JSON-LD payloads.

- The second draft of OpenID4VC was released in February 2025.

Authentication & Authorization

- OAuth-protected APIs were discussed.
- Authentication will be based on the **issuer**.
- OpenID does **not** provide reference implementations for issuers.

HAIP Development

- HAIP will **not** be limited to SD-JWT and remains a work in progress.

Additional Topics Discussed

- Digital Credential API
- Custom URI scheme

Room L

How can we better include refugees in national systems?

Session Convener: Sam Jefferies, Andrew Hopkins

Specific Country / Technology Discussed:
Uganda, Niger

Tags / Themes of the session:
Refugee Inclusion, Interoperability, Data Sharing, UNHCR

Notes

- UNHCR presented the Ethiopia case study where the government worked with UNHCR and the world bank to change legislation and allow inclusion of refugees into the national digital identity programme.
- Ethiopia uses a MOSIP system for the Fayda ID, and UNHCR shares biometric data for cross comparison through interoperability, after which the Fayda is issued to refugees.
- There is value for states in inclusion and UNHCR is looking to support states and in particular identify states which have refugee data already with UNHCR which could be better included in state systems during any MOSIP digital transformation.
- A colleague from Burkina Faso expressed the need to better register and include IDPs in remote area
- Refugees are vulnerable & are looking to survive in their new country where they may be ethnically similar
- Data sharing policy with governments vs data protection & focus on de-duplication of identity
- Discussion on Somalia & Kenya: people registering for both systems, i..e National Registry & Refugee registry (asylum system)
- Interop predicated by data protection impact assessments;
- CRVS vs refugee system: how/where to register children, OpenCRVS wanting to collaborate in a use case in Uganda on children born to refugees when the children born here are legally residents of the country?
- Duplication of national & refugee systems
- Uganda has generously hosted many refugees
- Protecting data in vulnerable environments: staff led checks for fraud vs mistakes.

Room O

Implementing USSD Solutions for Resident Services and Grievance Handling: Ethiopia

Session Convener: NIDP Ethiopia

Session Attendees:
- Dagmawi Mekonnen
- Abel
- Biniyam Tedla
- Sanathkumar Varambally (MOSIP)

Specific Country / Technology Discussed:
Ethiopia , USSD implementation

Notes

Use Cases:
- Check Registration Status:
  - Allow users to check their registration status by using MOSIP's resident services API.

- Resend SMS (Lost UIN):
  - Provide an option to resend the Unique Identification Number (UIN) via SMS in case it is lost.

- Check Card Order Status:
  - Enable users to track the status of their card issuance.

Challenges:
- Session Time Limit:
  - Address the issue of sessions expiring too quickly, which can disrupt the user experience.

- Feature Phone Character Limits:
  - Adapt the system to work efficiently on feature phones, considering their limited character display.

Future Enhancements:
- Push Authentication:
  - Implement a secure way of verifying users through push notifications.

- Push Notifications:
  - Introduce real-time notifications to keep users informed about updates and actions.

Additional Notes:

- Togo's Interest:
  - Togo is exploring a similar solution, indicating a shared interest in leveraging these digital services.

- Payment Initiation:
  - Currently, payments are linked to the national ID. There's potential to integrate this feature in the future.

- USSD in India:
  - In India, USSD (Unstructured Supplementary Service Data) is commonly used for payment transactions, offering a model that could be explored further.

Room R

Finding Friends: Building Communities to Strengthen IDs

Session Convener: Kunal, Aapti Institute

Notes

- Increasing Adoption of Digital ID Systems:
  - Countries need strategies to drive greater adoption post-digital ID implementation.
  - In the Philippines, adoption remains slow due to **connectivity challenges** and a **lack of perceived direct benefits** for citizens.

- Enhancing Cross-Sector Collaboration:
  - Identified **use cases** that encourage collaboration between different sectors.
  - Recognized **duplication of efforts** due to insufficient communication across sectors and organizations.
  - Emphasized the need for **trusted data-sharing mechanisms** between systems.

- Encouraging Community Contributions to the Platform:
  - Discussed strategies to **increase open-source contributions** to the platform.
  - Explored ways to foster a stronger developer and contributor community.

- Next Steps:
- Identify **high-impact use cases** that demonstrate the benefits of digital ID to citizens.
- Develop strategies to **improve inter-sectoral communication** and avoid redundant efforts.
- Define a framework for secure and trusted data sharing between systems.
- Implement initiatives to attract and retain open-source contributors.

Room S

Overcoming Barriers to Last-Mile Financial Inclusion

Session Convener: Ed Cable

Tags / Themes of the session:
Definition of Financial Inclusion and Barriers to Digital Payment Adoption

Notes

Discussion Points:

1. **Definition of Financial Inclusion:**
    - The discussion moved beyond simple payment access to a broader concept of "financial empowerment" or "financial health."
    - It was emphasized that true inclusion involves access to a full range of services, including borrowing, saving, and insurance.
    - The need to enable people to meaningfully participate in and benefit from the financial system.

2. **Barriers to Digital Payment Adoption:**
    - Fear and Trust:
        - Concerns about digital payments being tracked, leading to increased taxation and privacy violations.
        - Lack of trust in digital systems compared to cash.
        - The need to show the advantages of digital payments.
    - Taxation and Fees:
        - High transaction fees and taxes on mobile money transactions were identified as significant deterrents.
        - The impact of these fees on small, frequent transactions made by last-mile users.
    - Digital Literacy and Device Access:
        - While smartphone penetration is increasing, concerns remain about access and equitable distribution of devices.
        - Social and Cultural barriers surrounding women's access to phones.
    - Behavioural and Psychometric assessments:
        - The use of non-traditional credit scoring such as behavioural assessments.
        - The difficulty of traditional financial institutions to accept these alternative forms of credit worthiness.

3. **Credit Worthiness and Access to Credit:**
    - Challenges in establishing credit worthiness for individuals with informal economic activity.
    - The need for alternative credit scoring mechanisms that capture informal financial behaviour.
    - The issue of financial institutions not recognizing credit data from informal savings groups.
    - The problem of predatory lending and the need for financial literacy to guide people to safe credit options.

- The need to educate individuals on when it is appropriate to borrow money.

4. **The Role of Technology and Digital Public Goods (DPGs):**
   - The potential of DPGs to provide modern systems for transactional accounts and payment services.
   - The importance of interoperability between mobile money rails and other financial systems.
   - The need for secure and transparent digital systems that build trust.
   - The importance of imitating the trust of cash into digital systems, such as the use of non-repudiation.
   - The need for authentication systems that are secure.
   - The need for systems that allow for constraints on payments.

5. **Government and Regulatory Challenges:**
   - The need for government policies that promote financial inclusion and reduce barriers to digital adoption.
   - Concerns about government priorities focusing on revenue generation over the needs of last-mile users.
   - The importance of training government officials on financial inclusion.
6. Social and Cultural Considerations:
   - Gender disparities in access to financial services and decision-making.
   - The importance of culturally sensitive approaches to financial inclusion.
   - The need to prevent digital financial tools from causing social harm.

Next Steps / Action Items:

- Develop strategies to build trust in digital payment systems, addressing concerns about privacy and security.
- Advocate for policies that reduce transaction fees and taxes on mobile money, especially for low-value transactions.
- Develop training programs for government officials on financial inclusion.
- Design digital financial tools that mimic the trust and security of cash.

Room U

National IDs at Scale:
Learnings from Hundreds of Use Cases in the Field

Session Convener: Venugopal M2P

Tags / Themes of the session:
Aadhar's success stories and drawbacks

Notes:

- Implementation and success stories of Aadhar.
- Drawbacks of Aadhar where DOB is never a source of truth. Aadhar is only a proof of identity (who is who)
- Discussion on the necessity of having National IDs and how it can ease service delivery.
- Discussion of one of the African countries where pilots of National ID are successful but actual rollout fails.
- Discussion on how Citizens enroll for a National ID only when they are informed well on the monetary and non-tangible benefits they receive.
- The use cases are often decided when there is greater impact and coverage across the country's population.
- Fraud can be identified by location bound, time bound and liveness bound detection.

Room V

Biometric-Based Identification for Small Countries

- Do we need biometric deduplication when the population is less than 1 million?
- Making SBI optional for enrolment: Challenges and consequences

Session Convener: Adam Cooper, Smita Selot

Specific Country / Technology Discussed:
Implementation of Biometric based Identification (SBI & SDK)

Tags / Themes of the session:
MOSIP for Small Countries, Biometric identification

Notes

The session explored whether biometric deduplication is essential for digital identity systems in countries with small populations or if alternative approaches could achieve similar objectives more cost-effectively.

Key Discussion Points

Challenges with Biometric Systems

- High implementation costs, especially for small countries
- Requirement for specialized hardware (high-quality biometric sensors and equipment)
- Need for robust software systems for biometric processing
- Staff training for biometric data capture
- Complexity and cost associated with biometric registration

Alternative Approaches Considered:

- Strengthening civil registration systems with thorough validation processes
- Social verification methods, such as community or church-based validation
- Phased implementation, starting with basic digital identity services
- Document-based verification with additional security layers
- Leveraging existing community structures for identity verification

Country-Specific Considerations:

- Implementation costs must be balanced against population size
- Assessing fraud risks across different verification methods
- Security requirements tailored to national contexts
- Long-term strategic planning (5-10 years horizon) for digital infrastructure
- Possibility of adapting successful models from other countries (e.g. Netherlands)

Practical Considerations:

- Need to evaluate trust in existing registration systems
- Balancing security requirements with convenience

- Option to start with distribution data analysis before full implementation
- Importance of accessibility for all community members
- Need for inclusive systems that work for marginalized communities

Implementation Strategy:
- Consider adopting a staged approach to digital transformation
- Plan for systems that can evolve over decades
- Begin with core functionality and expand services incrementally over time
- Evaluate specific country requirements rather than applying generic solutions
- Consider hybrid approaches combining different verification methods

Conclusion:
The discussion emphasized the importance of contextual solutions rather than applying uniform technological approaches across different countries, particularly for smaller population nations where implementation costs need careful consideration against potential benefits. For nations with smaller populations, careful evaluation of implementation costs and alternative verification methods is crucial to achieving a secure and inclusive digital identity system.

Room W

Navigating VCs

- Organization wallets and identities
- Navigating VCs- How do we plot the best course through the overlapping standards of verifiable credentials

Session Convener: Harmen, FIDES
Evan Miller, OpenCRVS

Notes:

. **Challenges for Issuers**

- Issuers often lack visibility into how and where their digital credentials are being used.
- Ensuring global acceptance of digital credentials, such as digital passports, is a key challenge.
- Different countries and organizations favor different credentialing standards, making universal adoption complex.
- The need to support multiple standards (e.g., MDL, MDoc) while ensuring compatibility across various ecosystems.
- On-premise hosting requirements significantly impact architectural decisions and implementation feasibility.
- Limited understanding and infrastructure for key management in certain regions.
- Parallel or siloed programs complicate the interoperability of credentials
- 2. Adoption of Standards and System Requirements
- The digital credentialing landscape is converging around a few key standards (approximately four to five major formats).
- OpenCRVS and similar systems must support multiple credentialing formats to cater to diverse regulatory requirements.
- Verifiable credential formats differ across regions, requiring flexible and adaptable implementations.
- Leveraging existing SDKs and tooling can expedite deployment and ensure compliance with prevailing standards.
- Organizational wallets, alongside personal wallets, can serve as API-driven solutions integrated into larger systems
- .3. Wallets and Their Role in Digital Credentialing
- Personal wallets (e.g., Apple Wallet, Google Wallet) are becoming more common, storing items such as boarding passes, tickets, and potentially digital IDs in the future.
- Organizational wallets serve different needs, potentially functioning as API integrations rather than standalone applications.
- Issuers (e.g., governments) provide credentials to these wallets, enabling identity verification and authentication.
- 4. Technical Considerations and Interoperability
- Overlapping standards and multiple SDKs are available to facilitate implementation.

- OpenID and similar frameworks are widely used for credentialing and identity verification.
- The need for standardization across issuers, holders, and verifiers to ensure seamless data sharing and authentication.
- Modular systems, such as those that use a certified module for data conversion and issuance, can help streamline credential management.
- Ensuring that digital credentials can be shared securely across different platforms while maintaining compliance with regulations

Next Steps / Action Items:

- Identifying low-hanging opportunities for adoption and standardization.
- Understanding the business value of verifiable credentials and how different stakeholders define success.
- Collaboration with specialists to refine standards, develop tooling, and enhance usability.
- Promoting interoperability and compliance to accelerate global adoption of digital credentials.

Session 3

Room B

Sharing Experiences in Brownfield Biometric Implementation

Session Convener: Ted Dunstone

Specific Country / Technology Discussed: Brownfield implementation and difficulties faced around the brownfield migration

Notes:

MOSIP Implementation and Data Migration Challenges
This discussion centers around the challenges and considerations for implementing MOSIP (Modular Open Source Identity Platform), particularly focusing on data migration from legacy systems and integration with existing government infrastructure. The participants, representing various organizations and countries, share their experiences and seek clarification on MOSIP's capabilities and best practices.

Data Migration Complexities
Ted Dunstone, from the Pixie Lab, initiates the conversation by highlighting the complexities of data migration in identity systems. He recounts an experience where a seemingly straightforward data migration for a national-scale system, initially planned for four weeks, ultimately took eight months with a 20-person team. This was despite migrating data within the same system, not even involving a platform change. Ted emphasizes the intricate nature of identity systems, with their associated metadata, analytics, and diverse stakeholder requirements, all contributing to the difficulty of data migration. He stresses the importance of careful data assessment, appropriate technologies, and robust infrastructure for successful migration.

UK Data Migration Challenges
Ted further illustrates the challenges of data migration with the example of the UK's attempt to transition from an older biometric system to a new architecture. This project, significantly hampered by data migration issues, ultimately failed. The complexity of the data migration proved to be a major stumbling block, leading to project failure and a change in vendors.

Data Quality and Deduplication
The discussion then shifts to specific data challenges faced by participants. Nambirajan, raises concerns about data quality and deduplication in foundational identity registries. They emphasize the need for quality checks and deduplication before migrating data to MOSIP. The current process is time-consuming, especially with large datasets.

Algorithm Training and System Functionality
Sam Jefferies, expresses interest in upgrading their biometric system and inquiries about MOSIP's suitability. They are particularly concerned about replacing their existing

bespoke system deployed at scale and seek insights into the experiences of other countries. They are interested in understanding the functional aspects of deployment and potential pain points.

Data Transformation and Integration
The conversation explores the technical aspects of data migration, including data transformation and integration with MOSIP. Nambirajan explains the process of extracting data from legacy systems, performing necessary transformations, and seamlessly integrating it with MOSIP. They also discuss the use of tools for data migration and the importance of addressing data format discrepancies.

Client Integration and Customization
The discussion delves into the integration of existing client applications with MOSIP. A participant describes a scenario where they converted existing data formats and pushed them into MOSIP's backend. The question arises whether to rebuild existing front-end clients for MOSIP or adapt them by adding a MOSIP connector.

Workflow Customization and Jurisdictional Access
Participants discuss the need for customizing workflows and managing jurisdictional access to data within MOSIP. The example of UNHCR's requirement to access data from multiple countries while respecting data privacy and jurisdictional boundaries is raised. The discussion also touches upon the challenges of searching across different databases for various purposes, such as missing persons databases.

Greenfield vs. Brownfield Implementations and System Integration
The conversation concludes with a discussion about the challenges of brownfield implementations and system integration. Participants share experiences with integrating MOSIP with existing non-MOSIP government systems. The need for a playbook or roadmap to guide countries through the implementation process is highlighted. The discussion also emphasizes the importance of system integrators and the need for capacity building within countries.

Next Steps / Action Items:

The key takeaways from this discussion include the complexity of data migration in identity systems, the importance of data quality and deduplication, the need for workflow customization and jurisdictional access control, and the challenges of integrating MOSIP with existing government systems. The participants agree on the need for more comprehensive guidance and support for countries embarking on MOSIP implementations, particularly in brownfield scenarios. A key outcome identified is the development of a playbook or roadmap to address common challenges and best practices.

Room D

How to bridge the gap between government-issued IDs and private sector authentication?

Interoperability of identity systems: Bringing PhilSys, MOSIP and other platforms together

Session Convener: Andrea

Notes:

Implementation Challenges

- Holland experiences limitations with national ID integration
- Lack of interoperability between systems is a significant barrier
- Common ground needed for interoperability across sectors (e.g., healthcare vs. finance)
- Legal restrictions around ID verification create complexities
- Switzerland still relies primarily on physical ID verification for government services
- Initial resistance to national ID adoption in the Philippines

Philsys Implementation (Philippines)

- The Philippine Statistics Authority (PSA) leads implementation
- Philsys has developed specific use cases for different sectors
- Partnership with DICT established for national ID e-verify system
- Different divisions handle government use cases, financial/private institutions, and social protection
- National ID is now accepted at banks
- 8 pilot programs with landline integration
- Philsys made significant efforts to enroll citizens through various initiatives
- Conducted outreach at airports and through collocations with other agencies

Success Factors

- Capacity building for institutions using national IDs is critical
- Private entity involvement is needed for ecosystem development
- Community building and education are crucial for acceptance
- Working through industry associations helps spread awareness (India example)
- India's approach: IBA (Indian Banks Association) and other associations conducted workshops
- Trust in the systems develops over time, not immediately

India's Approach

- Used interagency promotion (tax department promoted national ID)
- Identity Act governs how data can be shared and accessed
- Focus on all three stages of DPG (Digital Public Goods):

1. Identity ("who am I")

1. Credentials ("what do I have")
1. Services ("what can I do with it")

- Reduced costs for customer verification from $100 to under $5
- Private sector was allowed to innovate within boundaries

Rwanda's Approach

- Uses initiatives and hackathons to identify problems and solutions

Recommendations

- Educate citizens about benefits and data protection
- Allow citizens to be part of the system development
- Build trust through community engagement
- Encourage other agencies beyond Philsys to promote the system
- Private sector involvement will help improve authentication systems
- Need for decentralization of ID consumption
- Consider credential-based solutions to reduce centralized load
- Focus on sustainability and long-term benefits

Key Takeaways

- Education of citizens is paramount for acceptance
- Trust isn't built overnight—it requires time and consistent engagement
- System needs sufficient use cases to gain widespread adoption
- All stakeholders agreed that private sector involvement will help make authentication better

Room K

OpenID4VC conformance testing

Session Convener: Joseph Heenan

Specific Country / Technology Discussed:
OpenID4VC specifications

Links to Resources:
Presentation slides:
https://docs.google.com/presentation/d/1kygvpXOSu5a7zGN9Oq2ZzTeKhdo2DVd6/edit?usp=sharing&ouid=107381980093922120275&rtpof=true&sd=true

https://openid.net/developers/certified/

Notes:

Why OpenID
1. HIGH quality implementations

Open ID certificate
1. Financial grade API
2. Tests are developed with working group
3. Testers get support from domain experts
4. Interoperability problems can be found and updated
5. Anyone deployed using specific standards can run this
6. Doesn't check inside of wallet (secure)

Suite architecture
1. Multi party testing
2. Structured configuration
3.small piece of java code
4. Transparent process
5. Can be used in CI

Process to test wallet for verifiable presentations
1. Can be run locally
2. To get a Wallet certified mark. Run in Cloud.

Room L

Impact: What? How? Where?

Session Convener: Rohit Ranjan Rai

Session Attendees:

- Kunal Barua
- Abigail Faylor
- Sushant Kumar
- Kit Weaver
- Meghna Das
- Supriya Jambunathan
- Keerthi Shastri
- Tarun Cherian
- Swarathmika Kumar
- Anushka Sachan
- Nirupama Ganesh
- Mahek Sarkar

Tags / Themes of the Session

- What is the concept of impact?
- How do you measure impact?
- Where is the impact being seen?
- Why are we talking about impact?

Notes

What is Impact?

- Is it about numbers, or is it systemic?
- How do you measure impact? Is there a baseline?
- Where is the impact being seen, at the end-user level or at a national scale?

These questions have both policy and communication implications.

Why Are We Talking About Impact?

Our framing begins with the goals we want to achieve.
Namely:

- Making public services better
- Identifying the decisions needed to achieve this
- Demonstrating impact to the public, which expects accountability

There is an end user in impact, but countries have different frameworks than residents.
Attendee: Impact is positive change. What has improved or changed? It should be assessed at the citizen level. ROI is also a key factor and can be measured through impact.
There is a demand to capture impact to sustain philanthropy.

Purpose and Accountability in Impact

- We also need to ask, what is the purpose of measuring impact?
- Once impact is articulated, we become accountable for it. Example: Is MOSIP responsible for those 129 million IDs?

Attendee: Accountability is implicit in responsibility.
Deji: How did the ecosystem become invested in impact?

- It has to come from the context of the institution, to answer what is yours to do? That decides who the impact is for.
- Defining this helps determine who the impact is for and strengthens accountability.
- Value chains get blown up when people detach from the end goal — if everyone maps to the singular goal of resident impact it could encourage an unified end.

Measuring and Understanding Impact

- Chasing moving targets is an ongoing challenge.
- Primary and secondary levels of impact should be part of the conversation.
- A before-and-after perspective can be useful for measuring impact.
- Being removed from the end user leads to abstractions that may not reflect reality.
- Understanding our own role in the value chain is crucial to accurately assess impact.

Impact vs. Outcome

- Claiming attribution is important—impact must be a direct result of an intervention
- What are you claiming? Faster? Cheaper? More productive? If you measure what you claim, there would be the linkage to the outcome.
- Another question we need to consider: Are DPGs Responsible for Systemic Change?
- If we don't center the end user, we risk becoming supply-focused rather than demand-focused
- Where are we in the value chain? What are we triggering in the next stage?
- Unlike private tech, DPGs and DPIs contribute unique value with ripple effects on the ecosystem.
- The stories we tell shape the narratives we want to build around impact.

Next Steps / Action Items:

- Sushant: Communications should be tailored to the specific target audience.
- Meghna: Communications need bridge resources to provide enough evidence without exaggeration, and validate whether the problem is real.
- Keerthi: Talk about failures so that we can collectively learn from them.

Room N

How to Encourage Private Sector to Adopt DPI

Session Convener: Vinod, Mujir – CTO (Thoughtworks)

Specific Country / Technology Discussed:
- Nigeria
- Taiwan
- India

Links to Resources:
[Playbook for Digital Government]
https://www.thoughtworks.com/en-us/insights/e-books/digital-government-playbook

Notes:

Dr Michael - Taiwan, works at University
- working for ... researcher
- execution of Govt project - Digital Identity in Wallet (Credentials wallet to show to verifier)
    - sandbox would be there this month
    - Govt building infra
    - Next year, industry can run application in the infrastructure

- Post India Aadhaar enrolment, telcos authenticating leveraging Aadhaar was a good success story.
- Industry needs to think innovatively

Nigeria - National Payment switch - Industry (bank) - used ti to facilitate.. led to private sector involvement

Factors to encourage private sector involvement
- cheaper, faster and better
- willingness of Govt to trust and listen to private sector to adjust the regulation
- creating payment switch was an enabler for private sector involvement and innovation
- Companies need to find the best business model
    - Startups in India have done well leveraging DPI in their solutions e.g. PhonePe, GPay were newly created and disrupted the market in India.
- Not have over regulation
    - e.g. in Nigeria, there were stringent regulations to enable payments. Did not encourage fintech startups.
    - Big Banks leased the alliances to fintech startups, which was allowed by the regulators.
    - Banks got part of the transactions cost, 2 unicorns were created and citizens benefited from the innovation (PayStack - got acquired by Stripe, Flutterwave)
- Avoid inertia of not doing anything. This frustrates private sector
    - e.g. Nigeria - 180 out of 210 mil population
    - 40 to 110 million in 1 year, because Govt mandated that SIM should be attached to National ID

- Post that there were no specific initiatives to increase adoption
- cut back corruption, cost of services, linking social benefits to digital ID to bank account
- Tech that brings in some inclusivity for the country, in some countries supporting multi lingual. [Playbook for Digital Government](https://www.thoughtworks.com/en-us/insights/e-books/digital-government-playbook)

Sponsorship for Private sector
- pilot projects

How to convince end users to adopt the DPI? How secure is my data?
- data privacy law that is well enforced will increase the trust
- what do citizens do when there are incidents (e.g. unnecessary calls)
- increase awareness of people on good secure mechanisms to use DPI
- e.g. in India, not using phone numbers as UPI id, which increases chances of unsolicited calls.

Room O

Correctly Authenticating Citizens

Session Convener: Digvijay, Next Biometrics

Session Attendees:

- Anusha, MOSIP
- Suraj, MOSIP
- Sourabh, Thales
- Ashen Weerathunga, WSO2

Specific Country / Technology Discussed:

- Philippines
- India
- Peru
- Uganda

Notes:

Key Challenges:

- scalability/data sharing : all dept. collecting the same data multiple times, diff agencies following up
  - sometimes works in some part of the country but not in another
- depreciating quality of biometrics due to the age of the person
- device lifespan: tops out after 5years
- biometric spoofing/fake finger(registration & verification, focus is on verification)
  - cost for a liveness check
  - data being tamper proof during data capture, data transmissions, data storage/**MITM**
- beneficiary services collecting same biometric: i.e. tax dept & national registry both having/storing/needing duplicate info to register people
- consent: worry about sharing data (data law is different in every country)
  - E.g. Philippines residents don't want to give their biometrics for the registration phase
  - E.g. Peru incentivising enrollment via govt benefits
  - E.g. Uganda didn't have data laws; saving $20M year by spending $0.5M for enrolment, they mandated people to link SIM cards and gave 1 year deadline for the same
- data collection rate: not enough stations for collection
- identity validation: agencies in silos/
- UI/UX/operational challenges
- authenticating modalities

Solutions:

1. one number for all govt agencies, e.g. Tax dept
1. long time investment for biometric seeding of dependent dept.
2. biometric spoofing/MITM: L1 device
3. Fake finger detection

4. PAD-2 Certification.
5. Many ways to find the same end result, check what works for you
6. **Consent**: legal route, regulatory hurdle, can optionally incentivise registration with specific benefits.

Room R

Pricing for DPI Services

Session Convener: Ritul

Specific Country / Technology Discussed:
Sweden's **BankID model**, where banks jointly funded authentication infrastructure, shows private players should contribute to system maintenance.
The importance of learning from successful models and adapting them to local contexts was emphasized.
The case of Guinea was used as a good example of charging for services

Notes:

-Should the government charge the private entity?
-Who is the greatest beneficiary of aadhar? - Government
- Great products may not be free
- All services should not be always free, it may mislead the usage.
-Remote people who cannot afford , few transactions can be made free
- credit cards and master card company struggle in india due it's cost and surveillance

-The Aadhaar Authentication system has now been expanded beyond government and limited private services (like telecom and e-KYC) to include a broader range of private sector applications.
-This change raises questions about **authentication costs** as demand increases.
-A key concern was whether the pricing structure would be revised, given that more entities (e.g., e-bike rentals) can now use Aadhaar for secure identity verification.
-A **committee on pricing** was set up to determine the best approach, considering whether to charge based on **average cost** (total system cost divided among users) or **marginal cost** (cost per additional authentication).
Ultimately, **marginal cost pricing** was chosen to keep costs low while maintaining accessibility. For full **e-KYC authentication**, the charge was set at **₹20 (approximately ¼ USD)**, while **basic authentication costs ranged from ₹0.50 to ₹2**.
This decision aligns Aadhaar authentication with public infrastructure pricing models, ensuring affordability while maintaining financial sustainability.

- Digital Public Infrastructure (DPI) services should be charged or remain free, especially for private businesses benefiting from them.
- Many government-provided services (Aadhaar authentication, UPI, DigiLocker) are free, unlike private competitors like Visa and Mastercard.
- Aadhaar generates revenue, used for security improvements, but authentication fees are minimal.

Key Pricing Question: Should authentication services be free for public benefit or charged, especially for private businesses profiting from them?

1. **Aadhaar Authentication and Pricing in India:**

- The discussion began with the context of Aadhaar authentication in India, where the government has opened up its authentication services to more private services, leading to increased usage.
- The question arose regarding whether the authentication cost should be revised due to increased volume.
- India's approach was highlighted, with a committee on pricing considering average cost versus marginal cost.
- The decision to use marginal cost resulted in very low charges for authentication, while some services like UPI and DigiLocker remain free.
- The revenue generated is used to enhance security and infrastructure.

2. Should DPI Services Be Charged?

- whether DPI services should be charged to users or offered for free.
- Arguments for charging:
- Recouping costs of infrastructure development and maintenance.
- Ensuring sustainability of the services.
- Preventing abuse and overuse of free services.
- Creating a level playing field for private sector competitors.
- Value proposition to private companies that save costs by using the systems.
- Arguments against charging:
- Promoting digital inclusion and accessibility for all citizens.
- Maximizing public benefit and encouraging adoption.
- Recognizing the government's role in providing essential infrastructure.
- Savings that the government makes by having digital systems. (reduction of cash handling, direct benefit transfers)

3. Pricing Principles:

- Several pricing principles were proposed:
- Marginal cost: Charging only the cost of each additional transaction.
- Value-based pricing: Charging based on the value derived by users, such as cost savings or increased efficiency.
- Differential pricing: Charging different rates for different user groups or service levels (e.g., private sector vs. government).
- Usage-based pricing: Charging only for actual usage of the services.
- Pricing less than the alternate: if the citizen was to do the same task manually, then the digital version should be less expensive.
- Realizing the value: Government should make the users realize the value of the service.
- The importance of considering the impact on marginalized populations was emphasized.

4. Market Distortions and Unintended Consequences:

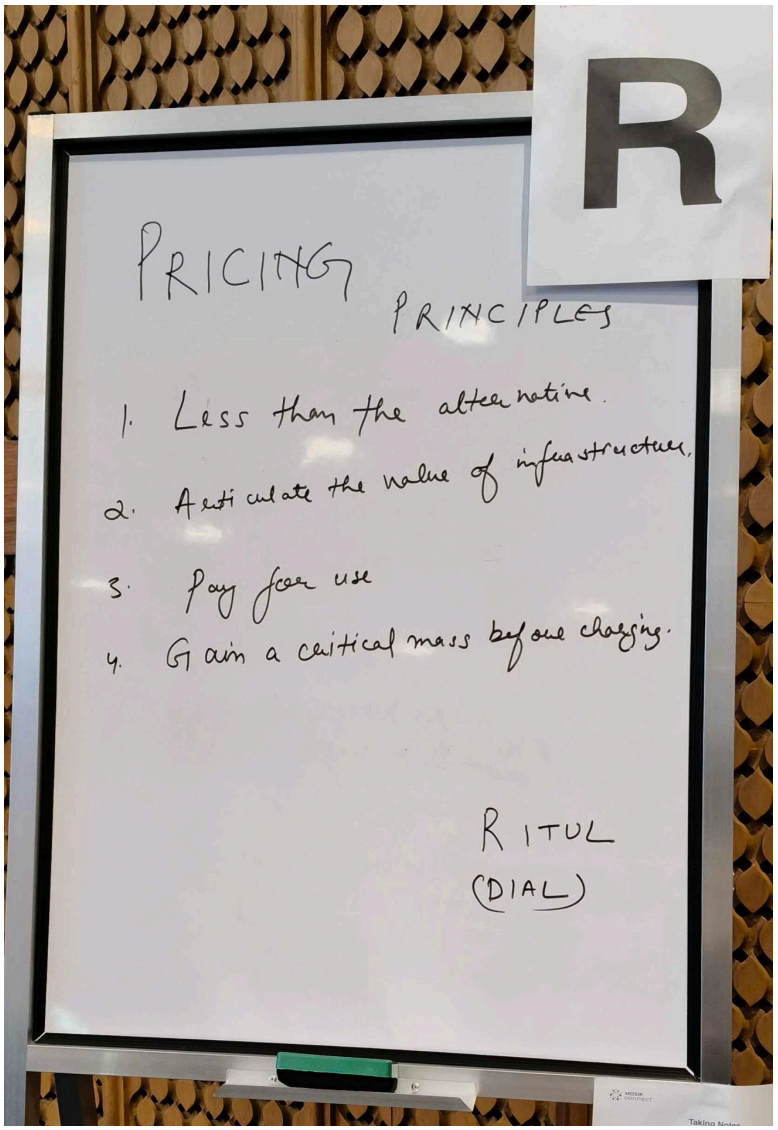
- Concerns were raised about potential market distortions caused by offering free DPI services.
- The government as a product developer can stifle innovation.
- Free services can lead to abuse, overuse, and security risks.
- It can discourage private sector investment and competition.
- The problem of third party verification companies not wanting digital systems.

5. Funding Models:

- Alternative funding models were discussed, such as consortiums of private sector players contributing to the cost of infrastructure.
- The Swedish model, where banks collectively funded a national authentication system, was cited as an example.
- The Indian payment corporation model was also mentioned.

6. Political Considerations:

- The influence of political factors on pricing decisions was acknowledged.
- The difficulty of implementing charges, even when economically justified, was highlighted.
- The need to communicate the value proposition of DPI services to both citizens and policymakers was emphasized.



Room S

DPGs Unleashed: Maximizing the Value of Implementing a DPG

DPI value with respect to economic development

Session Convener: Ed Cable

Notes

DPI and Economic Development:
Digital Public Infrastructure (DPI) has the potential to drive economic development by enabling more inclusive systems and creating livelihood opportunities. Various companies are contributing to this effort through two key factors:

- Inclusion and Livelihood:
  - Promoting access to education, training, and skill-building initiatives, especially in developing countries.
  - Empowering individuals with the skills required for digital literacy, financial inclusion, and participation in the digital economy.

- Reducing Economic Dependency:
  - Creating pathways for self-sufficiency through digital tools that support entrepreneurship, access to financial services, and improved market linkages.
  - Reducing reliance on traditional economic structures by encouraging innovation and localized digital solutions.

- Constraints Faced by Ministries:
- There are several challenges that ministries may encounter when implementing DPI at a national level:
  - **Lack of Incentives:** Ministries may not have direct incentives to solve these problems on a national scale, leading to fragmented efforts.
  - **Silos in Development:** Existing initiatives often operate in silos, making it difficult to create a unified approach. Breaking these silos is crucial for scaling DPI effectively.

- **Establishing Standards for DPG:** To ensure that Digital Public Goods (DPGs) align with broader economic development goals, standardized frameworks and strategies are necessary:
  - **Top-down Approach:** Identify key decision-making centers (power centers) and drive change through a top-down model to ensure alignment across various stakeholders.
  - **Collaboration with the Private Sector:** Leverage Corporate Social Responsibility (CSR) funds from private companies to support the development and implementation of DPGs.
  - **Engagement with External Ministries:** Make external ministries responsible for coordinating cross-border solutions and fostering global collaboration.

- **Building Functional DPGs:** Focus on creating functional DPGs that address real-world challenges, ensuring they have strong use cases that demonstrate value and scalability.

Room U

Cybersecurity for ID Systems

Session Convener: Shah Mahmood, The Alan Turing Institute

Links to Resources:

Cyber Observatory Trustworthiness Assessment Tool: https://www.turing.ac.uk/TDI/Cyobs
DISTAF: https://www.turing.ac.uk/TDI/trustworthiness-assessment-tool

Notes

All countries and ID systems
Splunk, Sentinel, and ELK are all log management and observability platforms that can collect, analyze, and store large amounts of data. The best choice for your country depends on the use cases, budget, threat levels and technical capabilities.
AI enabled Security Operations Center (SOC) for better monitoring
- SOC Level1 : Basic monitoring role
- SOC Level2: Incident response capabilities
- SOC Level3 : Expert level

Ukraine case study
- Data centers face threats from physical attacks, leading to the adoption of decentralized, cabinet-sized data centers. Key factors to consider include connectivity.

ID systems face constant attacks due to the high value of data as a target
- Rate limiting
- Security through obscurity (STO) is a security method that relies on keeping system details secret to protect it from attack. It's based on the idea that if attackers don't know how a system works, they'll have a harder time finding vulnerabilities.

DISTAF - Digital Identity System Trustworthiness Assessment Framework
- Self-assessment framework for measuring the levels of trustworthiness that an identity system achieves.
- Open-source framework

Cyber Observatory Trustworthiness Assessment Tool
- The Turing team has established a dedicated Cyber Threat Observatory to monitor and analyse threats in a timely way to empower identity system owners to be proactive in mitigating the increase in risks to the services that they offer.

Room W

MOSIP for Small Countries

Session Convener: Sivanand Lanka (MOSIP)

Tags / Themes of the session:
Lightweight version of MOSIP for smaller size population
MOSIP in the box
Light, ready to use MOSIP deployment
Small, distributed resilience

Notes

Key Discussion Points:
1. Why it is not suitable for small countries: Challenges for Small Countries Using MOSIP:
a. **High Cost Per ID:** Small countries face high per-ID costs, necessitating fine-tuning of the product for affordability.
b. **Infrastructure Footprint:** Countries require flexibility in MOSIP deployment based on their specific infrastructure needs.
c. **ABIS Installation Costs:** 70-80% of costs are attributed to ABIS installation, highlighting the need to optimize deduplication and biometric processes.
d. Simplifying MOSIP Architecture:
  i. Reducing the deduplication stage.
  ii. Exploring the possibility of removing biometrics for smaller populations.
  iii. Reducing storage footprint and exploring cost-effective alternatives.
e. Infrastructure and Capacity Planning:
  i. Need for a detailed recommendation on infrastructure requirements based on population size.
  ii. Providing predefined deployment configurations to ease adoption.

2. Technical Optimizations Discussed:
a. **Encryption & Data Compression:** Exploring ways to reduce packet size and optimize storage.
b. Strategic Storage Optimization:
  i. Shifting from SSD to lower-cost databases post-registration.
  ii. Exploring Claim 169-based storage solutions to reduce biometric storage requirements. Currently, MOSIP extracts the biometric template, while IDA stores the associated data. The biometric data is retained within the packet, allowing it to be used for regeneration when needed.
c. Simplified Deployment – 'MOSIP in a Box':
  i. A pre-configured, lightweight solution for easy deployment without heavy infrastructure.
  ii. Ensuring seamless integration with other **DPGs** for broader interoperability.

3. Existing Solutions & Next Steps:
  1. **Multi-Biometric Considerations:** Identifying cost drivers in partner countries and working towards cost-effective solutions.

2. **Sandbox Complexity & Optimization:** Exploring ways to simplify and reduce infrastructure overhead for sandbox environments.
3. **Automated Configuration:** Ongoing work (led by Alan Turing) on automatic configuration to further minimize MOSIP's infrastructure footprint.
4. Guidance for Countries:
   i. Providing clear guidelines on configurable options.
   ii. Helping countries design their identity systems based on what can be optimized without compromising functionality.

Conclusion: The discussion emphasized the importance of adaptability, cost efficiency, and technical optimizations in making MOSIP more accessible to smaller countries while maintaining security and functionality.

Room X

Last-Mile Enrolment in Challenging Geographical Location through Android MOSIP Client

Session Convener: Ankush Soni

Session Attendees:
- Nicole Navea (PSA)
- Pragya Kumari (MOSIP)
- Sanchi Singh (MOSIP)

Specific Country / Technology Discussed:
TFT Scanner for Capturing Fingerprints on Android Platform
Mobility offerings for Enrolment Kits

Tags / Themes of the session:
Ease of Enrolment
MOSIP Enrolment on Android

Notes:

- Discussed the challenges with respect to size and weight of Enrolment Kits.
- Issue of multiple trips to remote places with enrolment kit in case of issues with enrolment
- Use of AI in detection of fingerprints which are difficult to capture
- Benefits of using Android Registration client on Tablet/Handheld with TFT scanning technology
- Use case for Enrolment Scanners as authentication devices with L1 specifications

Unanswered Questions:
Challenging segment with currently available tablets with only one USB/connectivity port option

Next Steps / Action Items:
Work to overcome current restriction in Android devices for connecting multiple devices through USB Hub concurrently

Session 4

Room D

Cross-Border ID/Certification Service with Partners

-Turing space in Taiwan
-How to improve it?

Session Convener: Henry Hang

Specific Country / Technology Discussed:
Taiwan / Verifiable Credentials

Notes:

- Verifiable Credentials (VCs) in College & Academic Credentials
  - VCs are increasingly being used for college and academic credentials, enabling seamless verification across institutions and borders.
  - Standards such as OpenIDVP (OpenID for Verifiable Presentations), OpenIDVCI (OpenID for Verifiable Credential Issuance), and SD-JWT (Selective Disclosure JWT) are widely adopted.
  - These standards ensure interoperability, security, and privacy when issuing and verifying academic credentials across different platforms and institutions.
- Schema Standardization & Conversion Across Countries
  - Different countries use varied credential schemas, which can create challenges in cross-border VC adoption.
  - A conversion tool can be developed to facilitate the mapping and transformation of credential schemas between different country formats.
- Trust Building for Cross-Border VCs
  - Establishing trust frameworks between countries is crucial for enabling cross-border VC usage.
  - Agreements and interoperability protocols can ensure that credentials issued in one country are verifiable and accepted in another.
  - Potential use cases include travel, education, healthcare, and employment verification.
- Decentralization of National IDs vs. Certificates
  - Discussion on whether National IDs should be decentralized or managed by a central authority while ensuring VC-based verification.
  - Certificates (such as education credentials and professional licenses) may have a more flexible decentralization model, allowing issuers to define their validation mechanisms.
  - The debate continues on the balance between decentralization and regulatory compliance.
- Cross-Border ID Usage and Current Developments

- Cross-border VC adoption is a growing interest among governments and private entities.
- Taiwan's Approach: Taiwan is exploring VC-based ID verification for international use, looking at interoperability and trust mechanisms.
- Other countries are also evaluating how VCs can enable seamless identity verification for international mobility.

- Inji Protocol for Issuers
- Inji Protocol can play a crucial role in VC issuance and verification by providing a standardized framework for issuers to adopt.
- Encouraging governments, academic institutions, and financial entities to integrate with Inji Protocol for cross-border credential verification.
- Ensuring scalability, security, and compliance with global standards.

Next Steps / Action Items:

1. Strengthen adoption of VCs for academic and professional credentials using governmental wallets and personal wallet
2. Develop a **conversion tool** for schema compatibility across different countries.
3. Work on trust frameworks to enable seamless cross-border VC verification.
4. Explore **Taiwan's model** and how it can inform broader cross-border VC adoption.

This discussion will guide future developments in VC interoperability, cross-border identity verification, and decentralized credentialing models.

Room F

MOSIP Deployment: Lessons Learnt and Returns of Experience

Session Convener: Eric Gresteau

Specific Country / Technology Discussed: Uganda, Morocco

Tags / Themes of the session: MOSIP Platform Deployment

Notes:

Key Discussion Points:
Version Upgrades and Automation Challenges

- Transitioning from V2 to V3 is difficult due to multiple changes.
- Need for increased automation in deployments.
- Discovery of which service talks to what is tedious and unclear.

Reference Architecture & SLAs

- Need to collect more feedback on deployment challenges.
- SLAs cannot be agreed upon effectively with the DC team.
- The Reference Architecture (Ref Arch) needs to be defined and finalized.

Schema and Compatibility Issues

- Schema complexity (140 fields) makes workflows challenging.
- Having to maintain a single schema doc can be challenging, if a new workflow can be added where this can be broken down into use case specific schema.

Upgrade Process & Versioning

- Upgrades are hard, leading to issues with versioning.
- Transitioning from GitHub to Bitbucket raises concerns about repository migration (country specific concerns).
- Teams are building their own images; need better workflows and documentation.

Training & Documentation Gaps

- Training duration of 3 weeks is insufficient to cover all deployment aspects.
- Documentation is unclear, especially on upgrading and compatibility.

Environment-Specific Challenges

- Sandbox vs. Production environments are significantly different.
- Network zoning is not clear, especially in production.
- Registration client (Reg Client) and reference integration details are not well-defined.
- The DC team manages Network & Security Zoning, but the process needs more clarity.

Production Deployment Issues

- Port mapping is unclear in the production setup.
- Nginx is used for routing, but configurations are not well documented.
- Understanding how services communicate (Kernel, PMS, and other flows) remains a challenge.

Country-Specific Observations

- Uganda: Need to share more deployment experiences and guides.
- Morocco: Service communication and deployment flow need better clarity.

Next Steps & Action Items:

- Improve documentation on schema, workflows, and upgrade processes.
- Enhance training programs to cover more deployment scenarios.
- Clarify network zoning and security practices, especially in production.
- Provide better guides on service communication and port mappings.
- Develop migration strategies for repository transitions (GitHub → Bitbucket). (useful for countries not dependent on github actions for build process)
- The creation of Ref Arch should involve community input, with outcomes documented in white papers.

Room G

User Experience vs Best Practice vs ID Inclusion

Session Convener: Priyan from Bevolve

Tags / Themes of the session:
Balancing User Experience and Best Practices
Inclusion vs. Data Integrity
Data Migration and Legacy Systems
Digital Identity Implementation
CRVS Systems

Notes:

1. **Balancing User Experience and Best Practices:**
   - The core issue revolved around requests from governments to simplify systems for user convenience, often at the expense of established best practices and data integrity.
   - Examples included:
     - Requests for simplified registration processes that might bypass necessary verification steps.
     - Demands for direct API access to sensitive data, such as national ID numbers, through simple name searches.
     - The need to balance the convenience of self-registration with the necessity of robust identity verification.
   - The challenge of accommodating populations with limited documentation or digital literacy.

2. **Inclusion vs. Data Integrity:**
   - The tension between ensuring inclusivity (reaching marginalized populations, migrants, refugees) and maintaining the integrity of the data collected.
   - The difficulty of providing digital IDs to individuals without traditional documentation.
   - The need for flexible registration processes that accommodate diverse circumstances.
   - The need to have systems that can handle edge cases.

3. **Government and Political Challenges:**
   - Political will and inter-ministerial coordination were identified as critical factors.
   - Lack of clear legal frameworks and policies to support digital identity initiatives.
   - The impact of political changes and shifting priorities on project continuity.
   - The need to educate the government on the importance of best practices.
   - The problem of different ministries having different systems, and the need to consolidate.

4. **Data Migration and Legacy Systems:**
   - The complexities of migrating data from legacy systems to modern digital platforms.

- Challenges related to data quality, duplication, and the absence of essential data fields (e.g., email, phone number).
- The need for robust data cleaning and migration strategies.
- The problem of migrating biometric data.

5. Biometrics and Authentication:

- Discussions on the use of biometrics (fingerprints, iris scans, facial recognition) for identity verification.
- The need for flexible authentication methods to accommodate individuals with varying biometric capabilities.
- The use of introducers to help people that do not have traditional documents.
- The need to educate users on the security of biometric data.

6. Operational and Logistical Challenges:

- The sheer scale of national identity projects and the logistical challenges of reaching large populations.
- The need for effective distribution strategies for digital IDs.
- The importance of public awareness campaigns and user education.
- The problem of people not wanting to get national IDs.
- The problem of people having multiple SIM cards, and the need to tie them to a national ID.

6. Configuration and Customization:

- The importance of flexible and configurable systems that can adapt to the specific needs of different countries.
- The ability to customize registration processes, data fields, and authentication methods.
- The need to have systems that can handle different date formats.

8. The Role of System Integrators (SIs):

- The crucial role of SIs in bridging the gap between government requirements and technical implementation.
- The need for SIs to educate government stakeholders on best practices and potential trade-offs.
- The importance of strong communication and collaboration between SIs and government agencies.
- The need for SIs to understand the legacy systems of the client.

Room K

Hybrid Hosting Option for Rapid MOSIP Deployment

Session Convener: Pete Herlihy (AWS)

Specific Country / Technology Discussed:
AWS Outpost offering was discussed for Country needs where they don't have AWS region or data centres in their country.

Notes:

- Countries are usually averse to going to the cloud – concerns around data security and sovereignty
- Most countries see it as a binary choice between cloud and on-prem – but it's a spectrum
- If you don't have AZs in your country, AWS are introducing "outposts" - if you don't have a local zone in your country, the outpost offering can start as small as a single server and grow as much as you want, and they are 'managed servers' by AWS put into your own datacenter (so you have to provide power, cooling, etc.). It allows you to access Cloud services and benefits like 'regions' even if you don't have a region near you (which includes things like security in access control). The outpost is Amazon property and it is not allowed to be tampered with. It is the data inside that belongs to the gov.
  - Database; Compute; Storage (S3) - is all within the datacenter
  - Regional connectivity is used for IAM control
  - Even the chips on the servers are partitioned so that one portion of the chip is used to connect to AWS 'control plane', and the rest can be used for customer data, etc.
- Starting at $500 per month for a server. A vehicle will deliver the servers, and you can be up and running very quickly.
- MOSIP can run on an outpost - it's a step towards 'MOSIP in a box'
- With an outpost, if you lose internet connectivity, you lose access to the control plane, so you lose access to your outpost – so, they've added satellite connectivity fail-over.

Discussion:

- An advantage of Cloud is the possibility of being able to easily upgrade hardware. How does this work?
  - These are managed servers so they will be replaced - patching, rotation of devices, etc. is all done by AWS.
- You could have 2 resources within the country and set up DR (disaster recovery) between the two. You could have 'active-active'
- But there is also a minimum set of network requirements - but Sanath says that's needed for MOSIP-adopting countries anyway.
- If AWS can't operate in that country anymore, does the server become unusable for the government?
  - It would need to be a migration. Obviously if it happened quickly, you would lose access. So this would need to be part of the recovery plan.

- Lock-in is a concern. But Pete argues that you're locked into anything to some degree. - instead, think about the cost of change
  - AWS would advise Govs to understand their portability options before they choose where to put their solution
- The other concern is about the FBI accessing the data (particularly since the passing of the Cloud Act). But the data is encrypted and only the customer has the keys.
  - Also, the ability to provide the scale in a cost-effective way, is a challenge. An example is UPI and companies like PayTM bringing workloads onto government servers that were completely unexpected when the thing was conceptualised.
- AWS, on contract end:
  - Since you own it, if you want to move out you can – but note that data out has a cost, but data in doesn't
- If you want to upscale though, you will need to have resources outside the country. That is the limitation of the outpost. So if you had a big registration drive for some reason, you might need to make use of compute and storage outside the country. You could architect it to allow this in situations of exceptional demand.
- How do you prove the security of the managed server? Can the customer do penetration testing etc.?
  - Pete: There's 'closed-box testing'. There's also independently-audited documentation available to customers.
- Arguing that the outpost is going to be more expensive than cloud but still significantly cheaper than running your own equivalent system.
- It costs $7 billion for AWS to build a region – so they're never going to build a region in every country.
- The control plane is *of the outpost*. The rest of the infra is controlled by your own IAM system.
- Not *all* Amazon services are available from outpost - S3, EKS, RDS, Compute, etc. … (see online)
- The value:
  - The protection (Cloud front etc.)
  - The regional support
  - Speed of delivery and the fact that the devices are managed
- Cost for outpost: you commit to a certain length of time, which has an infra cost. But then if all the things you put on are open source (e.g. the OS, etc.), then you have no extra cost. But any additional licenses, or managed service fees would have a cost. If you subscribe to Direct Connect, there is no extra cost for ingress and outgoes.

Room L

Civil Registration + ID Achieving Secure Delivery Excellence

Session Convener: Annina Wersun, OpenCRVS

Session Attendees:

- Philippines
- Uganda
- World Bank

Notes:

End-to-End Identity Management (E2E):

- Implement a seamless identity lifecycle from birth to death.
- Integrate civil registration and identification systems to ensure continuous identity tracking and secure service delivery.**2. Frontline ID From Birth:**

Establishing ID at Birth:

- Assign a unique ID at birth, ensuring every citizen is recognized from the start.
- Link this ID to vital events throughout a person's life for better governance and service delivery.

Key Use Cases:

- Service Delivery From Birth:
  - Enable immediate access to healthcare, education, and social services.

- Senior Citizens:
  - Facilitate pension distribution, healthcare access, and other welfare programs.

- Simplifying Governance:
  - Provide governments with a reliable mechanism to track citizens and streamline service delivery.
  - Reduce duplication and fraud by creating a single source of truth.

- Inclusion of Indigenous People:
  - Develop tailored strategies to include marginalized communities in identity registration processes.
  - Address challenges like geographical isolation, lack of documentation, and digital literacy.

Linking Vital Events:

- Integrate life events such marriage, and death with the ID system.
- Ensure timely updates to the ID system as these events occur to maintain accuracy.**5. ID Deactivation:**

When Should the ID Be Deactivated?

- Deactivate the ID upon the person's death to prevent misuse.

Role of CRVS (Civil Registration and Vital Statistics):

- Use the CRVS system to verify life events and ensure IDs are deactivated appropriately.

Case Study: Uganda's Integrated System: Uganda has successfully integrated Civil Registration (CR) and Identification (ID) systems, providing a robust model:

- Birth Registration:
- IDs are assigned at birth in hospitals, creating a foundational identity.
- Biometric Updates:
- Biometric data is updated at age 5 when the child starts school.
- Physical ID Issuance:
- Physical IDs are issued at this stage to facilitate service access (e.g., education, voting).
- Marriage and Death Records:
- Marriages are recorded to update the ID.
- IDs are deactivated upon death, ensuring accuracy in citizen records.

Key Considerations:

- Establish clear guidelines for when and how IDs are updated or deactivated.
- Leverage technology to create a smooth flow of data between Civil Registration and ID systems.
- Ensure privacy and security while enabling data-sharing mechanisms across government agencies.

Room O

Ensuring Biometric And Data Quality In Real Systems

-Operations
-Data migration

Session Convener: Ted Dunstone

Session Attendees:

- Dmitry Morozov
- Zeeshan, MOSIP
- Abdul bathish , MOSIP
- Nithya, MOSIP
- Janardhan, MOSIP
- HARMEN VAN DER KOOIJ, FIDES
- SOURABH -fron THALES
- Suraj- MOSIP
- Anusha
- Janardhan
- Rakshith
- Rajeev
- Nambirajan
- Suraj
- Lenah

Notes:

Introduction to Biometric System Quality
The speaker begins by discussing a recent session in France, where they explored the importance of biometric data quality. They emphasize three essential aspects that determine the effectiveness of biometric systems: accuracy, vulnerability, and quality. Accuracy refers to the system's ability to correctly identify individuals, while vulnerability addresses the system's resistance to bypass attempts such as photos or fake data. Quality is considered crucial because without good quality data, accurate matching and vulnerability detection become ineffective.

Defining and Exploring Quality in Biometrics
The speaker stresses that quality is often overlooked, but is critical to a biometric system's success. Quality can be influenced by multiple factors, including how the user interacts with the device, such as whether they are pressing the device too hard or aligning themselves correctly with the camera. Additionally, environmental factors like humidity, lighting, or other external conditions can affect quality. The speaker notes that achieving consistent quality is challenging because different areas can have varying levels of quality due to factors like operator expertise or environmental conditions.

Introduction to Speaker and Team
The speaker, Ted, introduces himself as the CEO of Multipixie Lab, a company specializing in testing and assurance for biometric systems. He mentions that the lab also produces open-source software called VCAT, which integrates with MOSFET and can be used

independently as a standard package. After this introduction, there's a brief round of introductions from the workshop participants, highlighting diverse locations including Mosul, Dallas, and Udalla.

Workshop Structure and Focus
Ted outlines the structure of the workshop. The first part will focus on discussing the general concept of quality in biometric systems, and he encourages participants to share their experiences. He explains that quality is multi-dimensional and involves factors like user interaction with the device, device performance, and the surrounding environment. Demographics also play a significant role in determining how effective biometric systems are, especially when considering different skin tones or medical conditions that may interfere with biometric capture.

Challenges in Biometrics: Demographics and Device Limitations
Several specific challenges are mentioned, including how certain populations may face difficulties with biometric systems. For instance, individuals with very light or dark skin might pose issues for camera sensors that rely on contrast. Similarly, fingerprint sensors often struggle with users who have hand sanitizer or lotion on their fingers. An example is given from a country in the Pacific where high rates of diabetes meant that many citizens could not provide usable fingerprints, highlighting the importance of considering demographic factors when implementing biometric systems.

Quality Measurement and Management
The discussion moves to the practical aspects of managing and ensuring quality in biometric systems. Quality control starts at the device level, where parameters are set to ensure the capture of usable biometric data. If the quality settings are too strict, some users may be excluded, even though they have valid biometric data. The importance of providing user feedback during enrollment is stressed; for example, a fingerprint sensor should provide guidance on whether the finger placement is correct. Ted then discusses the various stages where quality checks can be implemented: at the device level, during enrollment, at a workstation where data is manually reviewed, and at the central database where data is stored. Each stage offers an opportunity to identify and correct poor-quality biometric data.

Challenges in Maintaining Consistent Quality
Ted explains that, over time, it is essential to monitor and ensure the consistency of biometric data quality, especially in large-scale deployments like national ID systems. There can be significant disparities in the quality of biometric data captured at different enrollment stations, such as those in rural or remote areas. These discrepancies can lead to mismatches in the system, so it is important to sample data regularly and use the findings to improve future enrollments. This feedback loop helps maintain high standards across all enrollment stations.

Data Quality When Migrating to New Systems
When migrating biometric data to a new system, knowing the quality of the existing data is crucial. Some data may no longer be usable in the new system, or there may be opportunities to improve the data. Ted shares an example of work done with the Philippines, where data was sampled and quality parameters were analyzed to identify correlations with factors such as time, location, and demographics. This analysis helps

improve the quality of the system over time by identifying specific areas where the data may be lacking or require enhancement.

Discussion on Multiple Biometric Types and Security
The discussion turns to the use of multiple biometric types, such as fingerprints, facial recognition, and iris scans. Ted clarifies that while fingerprint-based systems are common, most national ID systems capture multiple biometrics to ensure reliability. In cases where one biometric type fails, others can often fill in the gap. However, challenges still exist when biometric data is of poor quality, and systems may need fallback options, such as passwords, to ensure reliability. The speaker stresses that biometric systems are not always perfect, and issues like false positives or incorrect recognition can occur.

Final Remarks and Challenges
The final portion of the transcript features a brief exchange about the importance of ensuring high-quality data in biometric systems. There is an acknowledgment of the challenges involved in capturing accurate biometric data, particularly when using single-frame features in certain systems. The discussion ends with some philosophical thoughts on the operational and design aspects of biometric systems, focusing on ensuring reliability and fairness while dealing with varying data quality.

Importance of Biometric Quality
- Biometric quality is one of three crucial pillars for high-performing systems:
    - Accuracy (matching the right person)
    - Vulnerability (resistance to spoofing)
    - Quality (essential for both accuracy and vulnerability)
- Quality encompasses biological, environmental, and device-related factors
- Poor quality data dramatically affects system performance (5% bad quality images can reduce accuracy by 40%)

Quality Measurement Points
- **At the device level**: Initial quality thresholds and user feedback
- **At the workstation**: Operator review and potential recapture
- **At central database entry**: Quality checks before storage
- **Monitoring over time**: Ongoing quality assessment across the system

Quality Factors and Challenges
- **Demographics**: Some populations have inherent challenges (e.g., Pacific nation with high diabetes affecting fingerprints)
- **Environmental factors**: Humidity, temperature, lighting conditions significantly impact capture quality
- **Operator training**: Critical but insufficient alone
- **Visual assessment limitations**: What looks good visually may be poor for matching (e.g., fingerprint ridge inversion)
- **Regional variations**: Quality can vary dramatically between urban and rural settings

Quality Assessment Tools
- **BQAT**: Open-source quality assessment framework that integrates various quality algorithms

- **NFIQ2**: Standard for fingerprint quality assessment (not optimal for contactless fingerprints)
- **RFIQ**: Emerging standard for face quality assessment (still in beta)
- Quality scores should be trusted over visual inspection

Best Practices

- Use multiple biometric modalities as fallbacks when possible
- Rely on quality scores rather than visual inspection
- Take a data-driven approach to quality assessment rather than anecdotal examples
- For brownfields implementations, profile existing data thoroughly before migration
- Be cautious with biometric enhancement as it can introduce artifacts
- Consider device certification through programs like MOSIP compliance testing

Key Considerations

- Quality algorithms continually evolve and improve
- Contactless and contact fingerprints have different quality assessment needs
- Balance between quality requirements and inclusion is crucial
- Digital signing at capture helps ensure biometric data integrity
- Detection of synthetic vs. real biometrics depends on having complete image data.

Room S

Challenges and Opportunities in Communicating Digital ID

Session Convener: Abigail Faylor

Notes:

Question 1: How would you explain the benefits of Digital ID to your grandmother?

- Ensures accessibility—makes it easier to access benefits and understand eligibility.
- Provides security—knowing where funds are located and that they are protected.
- Establishes identity—people will know who you are and what you qualify for.
- Offers proof of life—demonstrates existence.
- Validates at a human level—grants dignity and recognition.
- Digital format ensures it cannot be lost or separated from the individual.
- Consideration: What if someone does not want to be identified? While the impact of Digital ID is significant, it may not work for or be a priority for everyone.

Question 2: What one feeling would you like people to associate with Digital ID?

- Trust
- Security—confidence in accessing services
- Inclusion—recognized as part of the community
- Empowerment
- Safety
- Validation—proof of identity
- Confidence and peace of mind
- Sense of existence
- Documentation—feeling seen
- Ease of access and use
- Neutrality—should not impose barriers
- Opportunity—enables participation and connection

Question 3: What are the most challenging Digital ID questions that remain unanswered?

- How is data handled?
- What governance structures are in place?
- What are the different ID architectures, and how do governments and other entities access and use them?
- How does Digital ID prevent misuse by bad actors?
- Is Digital ID the only means of accessing social and other services? Why is it necessary?
- How can we ensure verification and authenticity?
- What if an individual does not want a Digital ID?
- Will it prevent identity theft?
- Do people actually care about data privacy, or is it primarily a first-world concern?
- If someone has multiple IDs, which one would they present first? Would a Digital ID be their preferred/first choice?
- How can we ensure Digital ID messaging is centered on user benefits rather than government efficiency?
- What is the unique value proposition of Digital ID?

Question 4: What communication tools and resources would be helpful?

- **Bridge resources**—provide visibility into the entire Digital ID ecosystem.
- **Visual systems**—icons or representations that clarify DPI and DPG elements.
- **User journey mapping**—showcase how Digital ID impacts individual lives, elevating real stories.
- **Personal accounts**—include perspectives on benefits and challenges.
- **Comprehensive access to data**—improve visibility into country-level information.
- **Interpersonal engagement**—foster deeper conversations on implementation and impact.
- **Clear, unified messaging**—develop a top 10 list of consistent responses to common questions.
- **Understanding ID system differences**—highlight how systems vary across regions, countries, etc.
- **Local context research**—what works in one country may not be effective elsewhere.
- **Evidence-based communication**—demonstrates what has been proven to work.
- **Use case descriptions**—show which implementations are successful and what resonates most with people.

Other Considerations

- Capture relevant analogies to simplify messaging.
- Advocate for additional funding specifically for communication efforts.

Room V

How can we leverage AI & LLM to improve localization, DPG or any software?

Session Convener: Jerome, OpenSPP

Links to Resources:

- https://www.odoo.com/
- https://openspp.org/

Notes:

OpenSPP: based on Oodo & OpenG2P

- Odoo: Popular open-source ERP
- OpenG2P

Brief discussion about LLM

- Problem area: lack of online texts of Laos
- took translation of LibreOffice and fed that to AI to improvise the translation
- used RAG to generate feed and generate better translation and then re-iterated
- Key result: got better translation using o3-mini & skipping Google Translation
- time to write the code: 3-4hours, saving 2-3weeks ago
- lower the temperature to make the AI less creative about generating the code

- AI gave a patch for the test, and later it got lazy and started giving patches for the business logic to make the tests pass
- lack of time to follow AI
- Grok, Mistral,
- open source, open weights, Neural network training can't
- Google Maps doesn't work in those 5% cases
- speaker's first year at school was re-writing libc, now students don't do C
- discussion on StackOverflow
- Cursor: discussion about it's costing $50/month with Claude's model.

Room X

National IDs at Scale: Learnings from Use Cases in the Field

Session Convener: Venugopal M2P

Tags / Themes of the session:
Aadhar's success stories and drawbacks

Notes:

- Implementation and success stories of Aadhar.
- Drawbacks of Aadhar where DOB is never a source of truth. Aadhar is only a proof of identity (who is who)
- Discussion on the necessity of having National IDs and how it can ease service delivery.
- Discussion of one of the African countries where pilots of National ID are successful but actual rollout fails.
- Discussion on how Citizens enroll for a National ID only when they are informed well on the monetary and non-tangible benefits they receive.
- The use cases are often decided when there is greater impact and coverage across the country's population.
- Fraud can be identified by location bound, time bound and liveness bound detection

Session 5

Room K

OAuth 2 security / interoperability / FAPI

Session Convener: Joseph Heenan

Specific Country / Technology Discussed:
FAPI 2.0 Specification

Links to Resources:
Presentation slides:
https://docs.google.com/presentation/d/1BnThT7FU1alQ9ZrBM-QUwBMaOaX-AWil/edit?usp=sharing&ouid=107381980093922120275&rtpof=true&sd=true

Notes:

1. Walkthough of the above presentation
2. Details were shared about the conformance test portal by OpenID foundation - Refer **https://www.certification.openid.net/**.
3. Any RFC for consent management APIs? - we were asked to refer Consent receipt specification by kantara initiative - https://kantarainitiative.org/download/consent-receipt-specification/
4. How is the client certificate shared with the resource server to verify? client certificate is shared in signed JWT header
5. Is it mandatory for all the banking solutions to adhere to FAPI 2.0? It is not yet mandatory all over the globe.

Room L

What can we do to include refugees in national systems?

UNHCR interoperability and data sharing

Session Convener: Sam Jefferies, Andrew Hopkins

Notes:

- Looking at generic interoperability with MOSIP
- Challenge currently faced in different countries is that the national identity registration and refugee registration are handled by different authorities, hence generating ID for refugees
- One of the countries is in hesitation to implement MOSIP due to the cost it requires to proceed. They don't want to deploy MOSIP using SI.

Room N

Web of Trust Map: What farmers, musicians, and realtors have in common about protecting their data?

Session Convener: Niza González, Nicholas Racz

Session Attendees:
- Libane Digital Economy minister
- (6 attendees)
- Daniel Goldscheider - Open Wallet Foundation
- Andreas Sigurdsson - ZADA Solutions

Specific Country / Technology Discussed:
Decentralised Identity in government and private sectors worldwide

Tags / Themes of the session:
Web of Trust Map
Decentralized Identity

Links to Resources:
https://www.weboftrust.org/
https://docs.google.com/presentation/d/1U04epYY43IelzZGtzWka0OEnrgspADJdsESJ7LEQO4g/edit?usp=sharing

Notes:

- A small overview of the digital identity systems was given. Starting from centralized systems like Aadhaar (India) to federated models like SingPass (Singapore, and now to decentralized identity, which intends to enhace security and user control.
- An important question to pose for this emerging technology: is it actually being used?
  - The **Web of Trust Map** is a unique effort to map out government-affiliated projects and individuals building the decentralized digital identity space. It highlights their connections, technology stacks, and protocols, offering a clear view of the ecosystem's exponential growth.
  - Through the research done on this map, government use cases where demonstrated, for example:
    - America: OrgBook (BC), USA Mobile Driver's License (MDL), QuarkID (Buenos Aires), Aruba Happy One Pass
    - Europe: European Digital Identity Wallet, Swiss e-ID, eZug, PosteID (Italy)
    - Africa: Mauritania e-ID
    - Asia-Pacific: Palau ID, Āhau, Bhutan NDID, Thailand NDID, sgID (Singapore), Seoul Wallet
- As proof that the technology is being used by the government, predominantly used as National IDs, wallets, mDL, a second question is presented: "Where is this technology also being used?"

- Agriculture (by farmers, buyers, intermediaries), real estate (by tenants or property managers), music industry (musicians), or education, finance, government, and many other industries.
- The main topic was to understand what farmers, realtors, and musicians had in common regarding their data, the result is they're all looking to have a secure, traceable, tamper-proof verifiable system.
- This understanding of what governments and what industries are using decentralized identity was identified through the Web of Trust Map.
- For an organization or project to be added in Web of Trust Map they can submit their information through the following form: https://airtable.com/appI8nn4WxgFaXkWp/shr98mLipidZlORvc or reach out to research@keystate.capital.

Room Q

Developing a Generic PKI Solution for ID

Session Convener: Sravunthy E + Praveen Kumar from BEL

Notes:

Demonstrate and discuss a novel PKI solution that leverages facial biometrics for enhanced security and privacy in identity management and secure communication.

Key Features and Concepts:

1. Face-Based Ephemeral Key Generation:
   - The core innovation is the on-the-fly generation of cryptographic keys using facial biometrics.
   - When a user presents their face, the system generates an ephemeral (short-lived) private key.
   - This private key is used to encrypt or sign data, and a corresponding public key is used for verification or decryption.
   - No biometric templates or personally identifiable information (PII) is stored.

2. Encrypted Packets and QR Codes:
   - Biometric data is not directly stored; instead, an encrypted packet containing relevant information is created.
   - This packet can be represented as a QR code for easy transfer and storage.
   - The QR code itself contains no raw biometric data.

3. Liveness Detection:
   - The system incorporates liveness detection to prevent spoofing attacks.
   - It verifies that the presented face is from a live person, not a photograph or video.

4. Decryption with User Consent:
   - The encrypted packet can only be decrypted with the user's live facial biometrics and, optionally, a PIN.
   - This ensures that data can only be accessed with the user's explicit consent.

5. PKI-Based Authentication and Authorization:
   - The system leverages PKI principles for secure authentication and authorization.
   - SSL certificates can be generated using facial biometrics, enabling secure logins and transactions.
   - It turns "biometric verification" into "photographic verification" using PKI.

6. Digital Signatures and Non-Repudiation:
   - Digital documents can be signed using facial biometrics, creating a strong link between the signer and the document.
   - The encrypted packet containing biometric information is appended to the document, providing non-repudiation.

7. Secure Communication:

- The solution enables secure face-to-face communication by encrypting and signing messages using facial biometrics.
- This protects against compromised systems and unauthorized access.
- Destruct pins can be used to display benign messages instead of the real message.

8. Blockchain Integration:
- The technology can be integrated with blockchain platforms, such as Hyperledger, for secure identity verification.
- It allows for verification of facial biometrics without storing sensitive data on the blockchain.

9. HSM Enhancement:
- Hardware security modules can be enhanced by encrypting stored private keys with the user's face, adding an additional layer of security.

Room R

Evaluating Models of Inji Wallet (VC) for Diverse Integration Needs

Session Convener: Vishwanath - MOSIP

Notes:

1. Decentralized model of INJI.
2. Explained how the loan portal uses different modules of INJI with demo video.
3. Detailing of each module(Inji Mobile Wallet,Inji Web Wallet, Inji Verify, Inji Certify) and VC specifications.
4. Overview of Claim 169 interoperability.

Room S

ID for Indigenous Communities

Session Convener: Jeremi

Specific Country / Technology Discussed:
- USA to Canada and vice-versa do not have any restrictions to travel between their countries without a National ID.
- Swedish "BankID" system: A cooperative digital identity system built by banks, which later became a national standard.

Notes:

When I have a passport, why do I need a National ID?

1. National ID & Digital Identity Inclusion
   - Importance of **inclusive identity systems** to ensure access to services, especially for marginalized communities.
   - Some individuals either lack a national ID or do not find it useful unless tied to social protection or benefits.
   - Example: In some countries, people prefer passports over national IDs for verification.

2. Challenges with Identity Systems
   - Some people struggle to obtain national IDs due to bureaucratic barriers.
   - Reports of Aadhaar issues in India, where some individuals faced difficulty accessing food due to lack of ID.
   - Countries like the **U.S. and France do not mandate national IDs**, relying instead on multiple identity documents (e.g., Social Security Number, passports, driver's licenses).

3. Trust in Government & Identity Systems
   - Some communities lack trust in centralized identity systems and prefer local identity models.
   - Example: Indigenous communities and regions with political instability may resist national ID registration.

4. Alternative Identity Approaches
   - Some **communities create their own identity systems** that may not be recognized by the government but serve local needs.

5. Social Protection & Digital Identity Use Cases
   - Identity systems are crucial for **social welfare programs** (e.g., food distribution, financial aid).
   - Issues of **fraud and favoritism** in social welfare programs where government officials register their friends or relatives.
   - Some local governments create their own identity lists, but implementation varies across regions.

6. Privacy & Security Concerns
   - Cases where lists of welfare recipients were publicly displayed, raising privacy and security risks (e.g., single women being easily identified).
   - Concerns about **data misuse** and ensuring digital identity systems **protect vulnerable populations**.

7. Role of Decentralized & Verifiable Credentials
   - Blockchain and verifiable credentials can help provide secure, tamper-proof identity records.
   - Localized digital identity solutions might offer **greater flexibility** for people who distrust central authorities.

8. Cultural & Ethical Considerations
   - Some communities (e.g., in **Mindanao, Philippines**) have cultural beliefs that restrict **photographing women** for identity purposes.
   - Government policies must balance technological advancements with cultural sensitivities.

9. The Future of Identity Systems
   - Debate on whether digital identity systems should be mandatory or voluntary.
   - Calls for **giving people the choice** to opt into national identity systems rather than forcing compliance.
   - In humanitarian aid, **alternative verification methods** should exist for those without national IDs.

10. Broader Philosophical Discussion
   - Some people **reject digital systems altogether** and prefer a **self-sufficient lifestyle** outside of formal identity structures.
   - Speculation on whether AI and automation may push people back toward simpler rural lifestyles in the future.

Room T

Government In A Box: Simple Integration of Open Source Solutions

Session Convener: Ted Dunstone, Ed Duffus

Notes:

- Challenges in deployment

- DPI in a box
- Gov stack cover all the use cases.
- OpenCRVS if we see gov stack we can take generic registration and turn into a civil registration and map potential solution

- Challenges in digital public goods
- Challenges in different sector
    - DPI in foundational and different sector

- Focus on minimal
- Show uses cases / impact potential
- Target small population countries

- OpenCRVS is on country level / region level -- its national level

- DPGs must be configurable

- Dpi in a box ? What should be in the box
- How tech benefit to him/her,how this effects the person/citizen
- How small population start the journey with what use cases what they started and how
    - Bhutan experience

- Focused on payment dpg can be deployed in 15 min and its very configurable and all the dependencies

- Demo data/country

- Connectivity should be in the box
    - Where do you send the data? Else we have very in efficient

- Who is the target audience ?
- Digital experts ? / figuring out the audience
- Responsible party for the use cases, its not a common component build
- Is it scalable ? If we can do for 1000 / it can be done for millions so this comes later.

Room U

Maximizing ROI of Digital ID Projects

Session Convener: Dmitry Morozov, 3DiVi Inc (Papillon Systems)

Tags / Themes of the session:
Cross-border Knowledge Transfer

Notes:

- Lowering the cost of enrollment
- Transfer knowledge from the more experienced country to less experienced country
- Telangana Govt is using this tech for criminal/forensic analysis
- Papillon Systems: Fully automated "KIOS" for identity enrollment

Room W

Asia Pacific Digital Identity Consortium (APDI)

- Cross border use case
- Boost synergies with Biz
- Trust framework and scheme

Session Convener: Henry

Links to Resources: https://www.apdiconsortium.org/

Notes:

APDI aims to promote digital identity in the Asia-Pacific region, develop cross-border efficiency and safety on data exchange, and prepare for sustainable growth of future technology.

APDI also wants to build business synergy for members and support the interoperability of verifiable credentials in the Asia-Pacific

- APDI's aim is to lead the development and implementation of standardized digital identity solutions, boost regional cooperation, and build trust in digital interactions in diverse industries.
- APDI consortium fosters trust and inclusion in digital identity across 36 countries
- In this session, they demonstrated how cross border use cases can be achieved with their trust framework and pre-defined schemas.

Goals of APDI:

- Build real country-to-country use cases
- Establish network-to-network messages
- Aim for real impact for people and the earth
- Build business synergies for members
- Develop cross-border services (banking, tax-refund, diploma)
- Support interoperability of verifiable credentials
- Propose digital identity framework
- Foster digital trust
- Bridge between Asia-Pacific and other regions
- Ensure access to digital services for everyone (inclusion)

Real Use Cases:

- Financial sector use cases
  - Verifiable Credential Interoperability (Enterprise to Bank, Bank to Bank)
  - Banking Innovation (Open Bank Account, Get Loan) - aiming for efficiency
- APDI connects different entities (issuers, holders, verifiers) through a gateway

APDI in 2025-2026:

- Goal: More countries joining, more members, more interactions
- More real use-cases, government involvement, and partnerships
- Acknowledging diversity in Asia-Pacific, aiming for a unique approach

Potential Questions

- Specifics of data format schema
- Details on the "gateway"
- Metrics for measuring "inclusion"
- How APDI will address specific cultural/language barriers
- Competitive landscape - are there similar organizations?
- Success metrics for APDI's goals.