DID:UNCONF AFRICA

Bridging the Digital Identity Gap in the SADC Region

FEBRUARY 18 - 20, 2025 | STIAS: STELLENBOSCH

BOOK OF PROCEEDINGS

February 25 - 27, 2025
STIAS / Stellenbosch Institute for Advanced Study
Stellenbosch, South Africa
www.didunconf.africa

Thank You Documentation Center/Book of Proceedings Sponsor: GLIEF

Contents

"As a non-profit organization, GLEIF has been a regular participant at the Internet Identity Workshop (IIW) since 2020, recognizing it as a vital platform for both learning and raising awareness about digital identity solutions.

IIW provides a unique opportunity to engage with the digital identity community on key initiatives, such as the verifiable LEI (vLEI), including its purpose, features, technical implementation, and governance framework.

The 'Open Space unconference' format of IIW offers a highly flexible environment, allowing sessions to be tailored for the benefit of both participants and stakeholders. Regionalization is a key pillar in GLEIF's new strategy, with a particular focus on the African subcontinent to extend onsite engagement and foster collaboration in the region.

GLEIF is honored to contribute to this inaugural event in Africa further strengthening global trust in the digital identity ecosystem."

About DID:UNCONF AFRICA

The intention of the event is to foster innovation and collaboration between emerging digital identity companies and projects across the SADC region.

About

The inception of DID:UNCONF AFRICA arose from the recognition that the SADC region holds immense potential yet faces unique challenges in digital identity. Our inaugural event emphasizes the vast disparities in the digital identity ecosystem and offers a stage for groundbreaking solutions tailored to the African context. DID:UNCONF AFRICA brings together thinkers, leaders, and innovators who are transforming the digital identity landscape, both locally and internationally.
Inspired by the collaborative and dynamic format of the Internet Identity Workshop (IIW),

DID:UNCONF AFRICA takes a more explorative approach, allowing participants to chart the course of discussions. The Open Space unConference format breaks the mould of traditional events, creating a space where every voice can be heard, from startups to industry giants. The event not only explores the intricacies of digital identity but also works toward weaving a cohesive network of innovators in the SADC region and beyond.

Event Background

DID: UNCONF AFRICA is inspired by the Internet Identity Workshop (IIW) that has been held twice a year, since 2005 in California for the global community working on Internet Identity. The longtime co-producer and Open Space facilitator of IIW Heidi Nobantu Saul collaborated with a local partner DIDx to plan and host the inaugural event. The second and third days of the event will be hosted with the same Open Space UnConference format that the Internet Identity Workshop has used for the past 20 years.

Thank You to our Sponsors!

What an unforgettable three days! To everyone who joined us—whether you flew in from across the continent or just down the road—thank you for showing up with such energy, openness, and curiosity.

Together, we explored what it really means to build digital identity for Africa, in Africa. From deep-dive sessions to spontaneous hallway debates, from big-picture policy to practical tech demos—**DID:UNCONF AFRICA 2025** was a space shaped by all of you.

To our incredible sponsors and partners: your support made this possible. To every speaker, facilitator, builder, and attendee—thank you for being part of the movement. This isn't just a conference. It's a community.

We can't wait to continue the journey with you in 2026!

3 Day Schedule

DID:UNCONF AFRICA 3 Day Schedule

Day 1 Kick-off: African-Focused Digital Identity Program
Tuesday February 18th / Doors Open at 12:30PM
Wallenberg Center at STIAS ~ Enter STIAS via Marais Road

ACTIVATING DIGITAL IDENTITY IN SOUTHERN AFRICA: WHERE ARE WE AND WHERE ARE WE GOING?

Arrival and Registration Welcome	12:30 -13:00 13:00 - 13:10	Keynote / "Digital Identity: A Global Perspective"	15:10 -16:25
Keynote/ Digital Identity: Where Are We & Where Are We Going?	13:10 - 13:40	Panel Discussion: "Interoperability and Scaling Digital Identity in Africa	16:25 - 17:10
Panel / Lessons Learned: From Identity Verification (ID&V) to Verifiable Credentials (VCs)	13:40 - 14:25	Keynote / The Future of Digital Identity	17:10 - 17:40
Private Sector Use Case: Twytch	14:25 - 15:10	Panel Discussion: Public Sector Identity Development in South Africa	17:40 - 18:00
Networking Break	15:10 - 15:40	Welcome Reception	18:00 ~

Welcome Reception in a relaxed and engaging environment directly following the end of the day

THANK YOU, OneVault & Secure Citizen, for making this possible!

Open Space unConference Day 2
Wednesday February 19 / Doors Open at 8:30
Coffee/Tea & Breakfast Snacks

Welcome & Introductions	9:30 - 9:45	Session 3	13:30 - 14:30
Opening Circle / Agenda Creation	9:45 - 10:30	Session 4	14:300 - 15:30
Session 1	10:30 - 11:30	Session 5	15:30 - 16:30
Session 2	11:30 - 12:30	Closing Circle	16:30 - 17:30
Lunch	12:30 - 13:30	Conference Dinner	18:00 - 22:30

Join us for a memorable Conference Dinner at the historic Middelvlei Wine Estate. Experience the charm of a traditional Cape Dutch setting while enjoying a delicious dinner and award-winning Middelvlei wines.
Complimentary transport will be provided.

- **Departure:** Buses will depart from STIAS at 18:00
- **Return:** First bus will return at 21:30 / and last bus at 22:30. Drop off will be Stellenbosch Town Centre from where delegates can walk to their hotel/guest house or book an Uber/Bolt.

Proudly sponsored by DIDx !

Day 3 Open Space unConference Thursday February 20 / Doors Open at 8:30 Coffee/Tea & Breakfast Snacks				
Opening Circle / Agenda Creation	9:30 - 10:00		Lunch	13:00 - 14:00
Session 6	10:00 - 11:00		Session 9	14:00 - 15:00
Session 7	11:00 - 12:00		Session 10	15:00 - 16:00
Session 8	12:00 - 13:00		Closing Circle	16:00 - 17:00
No Host Post Event Gathering / Suggested Location to be Announced				

DID:UNCONF AFRICA
Bridging the Digital Identity Gap in the SADC Region
FEBRUARY 18 - 20, 2025

Day 1 Kick-off: African-Focused Digital Identity Program

African-Focused Digital Identity Program
Through insightful presentations and dynamic panel discussions, we'll examine local challenges, emerging opportunities, and key innovations in the evolving landscape of digital identity in South Africa and the SADC region.

Theme of the Day:
Activating Digital Identity in Southern Africa: Where we are and where we're going?

This session will explore the current state of digital identity in South Africa and the SADC region through insightful presentations and engaging panel discussions, focusing on local challenges, opportunities, and innovations.

12:30 - 13:00
Arrival & Registration

13:00 - 13:10
Welcome Address
MC: Gideon Lombard, DIDx

13:10 - 13:40
Keynotes: "Digital Identity: Where Are We & Where Are We Going?"

Speaker:
- Shaun Strydom - Contactable

13:40 - 14:25
Panel Discussion: "Lessons Learned: From Identity Verification (ID&V) to Verifiable Credentials (VCs)"

Speakers:
- Jannie Pretorius - Secure Citizen
- Jason Shedden - Contactable

Moderator: Lohan Spies

14:25 - 15:10
"Private Sector Use Case: Twytch"

Speakers:
- Martin Grunewald - Secure Citizen
- Don Reddy - Twytch
- Varsha Gokool - Secure Citizen

15:10 – 15:40
Networking Break

15:40 - 16:25
Keynotes: "Digital Identity: A Global Perspective"

Speakers:
- Fraser Edwards - cheqd
- Shaveen Bageloo - Hashgraph Group

16:25 - 17:10
Panel Discussion: "Interoperability and Scaling Digital Identity in Africa"

Speakers:
- Karla McKenna - GLEIF
- Sam Henderson - YOMA
- Thokozile Mcopele - VISA

Moderator: Gideon Lombard

17:10 - 17:40
Keynotes: "The Future of Digital Identity"

Speaker:
Lohan Spies - DIDx

17:40 - 18:00
Closing Remarks & Call to Action
Gideon Lombard & **Heidi Nobantu Saul**

18:00
Welcome Reception in a relaxed and engaging end of the day. Thank You OneVault and Secure Citizen for making this possible

Day 2 & 3 Open Space unConference days

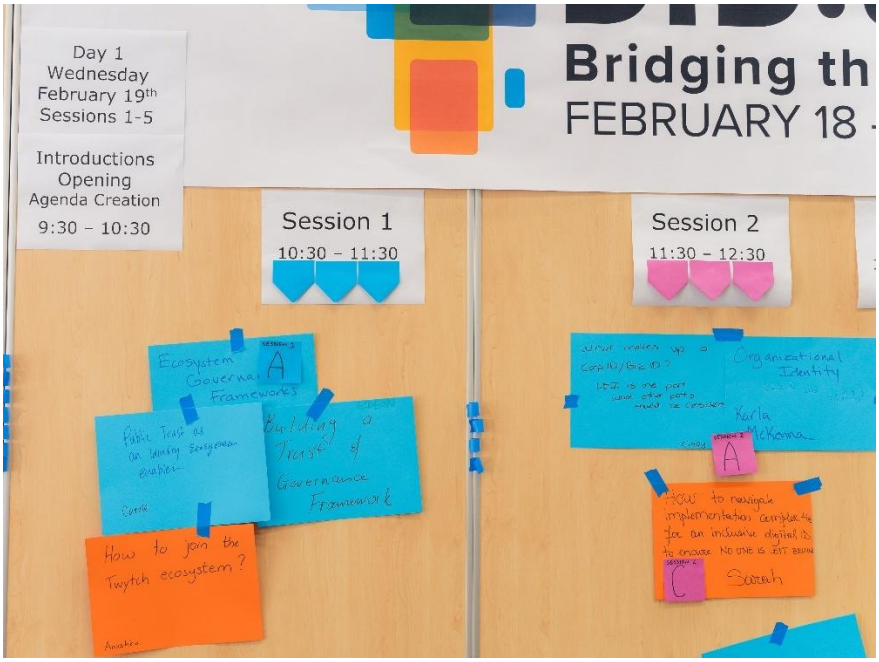
A two-day OpenSpace unConference
An immersive two-day exploration, inspired by the Internet Identity Workshop™ diving deep into the world of digital identity. We dispense with traditional keynotes, and engage in authentic collaborations through a co-created agenda. Examine the intricate facets of identity: people, organisations, and even the journey of products. Connect, track, support, and cross boundaries. Investments in standards, protocols, and systems find tangible applications here. Discover, Learn, Collaborate.

This is a participatory two days and it's all about exploring the agenda topics with professional peers from a range of identity areas. Like the Internet Identity Workshop, we will co-create the agenda together live each morning. The Open Space UnConference process will be professionally facilitated by Heidi Nobantu Saul the long-time co-producer and Facilitator of IIW.

Once agenda creation is complete there will be a full Agenda Wall of sessions posted, each with the time and place it will occur. Session topics are not voted on and all sessions put forth by participants at the start of each day will take place. Sessions are run as breakouts and attended by those who want to attend. There will be 5 session time slots a day, each with multiple concurrently running sessions.

Through multiple of sessions, lunches, a welcome dinner and a pre-event networking reception, provided by our generous sponsors (all included in the ticket), participants have plenty of opportunities to exchange ideas and make new professional connections. The Open Space UnConference format is perfect for a rapidly moving field where the organising team cannot predetermine what needs to be discussed, creating a space where every voice can be heard, from startups to industry giants.

Agenda Creation = Sessions Called and Hosted by Attendees



16 distinct sessions were called by participants and held over 2 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work for 14 of these sessions.

Day 2 / Sessions 1 – 5

Session 1
1A/ **These Sessions called separately chose to combine:** Building a Trust & Governance Framework / Gideon AND Ecosystems Governance Frameworks / Karla McKenna AND Public Trust as an Identity Ecosystem Enabler / Carrie
1B/ NO SESSION

Session 2
2A/ What makes up a Corp ID / Biz ID? ? LEI is one part - what other parts should be considered? / Cindy
2C/ How to navigate implementation complexities for an inclusive digital ID to ensure NO ONE IS LEFT BEHIND / Sarah
2D/ Back up and Recovery in a truly Self-Sovereign and Decentralized World / Robbie

Session 3
3A/ **These Sessions called separately chose to combine:** Financial Inclusion ID & Payments / Lohan S AND PAYSHAP: The Journey + where to next ? (interoperability, inclusion, identity ++) / Candice Mesk
3B/ NO SESSION
3C/ How do we get the government on board? / Merryl Ford

Session 4
4A/ Authoring DI for “Dummies” - Adoption (industry agnostic, individual, juristic, regulators) / Dalene Deale
4D/ Who has case studies? Let’s hear them! / Fraser Edwards

Session 5
5A/ NO SESSION
5C/ SA: Who isn't here but should be? / Fraser Edwards

Day 3 / Sessions 6 - 10

Session 6
6A/ The Role of Integrated Identity Platforms in the creation of DFIDs. Are they bound to one another? / Jason
6B/ NO SESSION

Session 7
7A/ Preventing 1984 / Willem Basson (This session took place in BO Space F)
7B/ NO SESSION

Session 8
8B/ **These Sessions called separately chose to combine**:Standards? Reuse? Redo for Africa? / Shavean AND The future of OID4VC & DIDComm / Max Coleman
8C/ NO SESSION
8E/ Levels of Assurance / Gideon L

Session 9
9A/ Delegated Authority & Attestation Attributes / Karla and Carrie
9B/ NO SESSION
9E/ Decentralized Smart Proxies / Lohan

Session 10
10A/ How to join the Twytch ecosystem? & Is the tech ready to demo and/or use? / Anushka Soma-Patel

Session Notes / Wednesday February 19/ Sessions 1 - 5

SESSION #1

Session 1A

Building a Trust & Governance Framework - Ecosystems Governance Frameworks - Public Trust as an Identity Ecosystem Enabler

Session Convener: Gideon L, Karla McKenna, Carrie
Session Notes Taker: Gideon Lombard and Karla McKenna

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Notes for Ecosystems Governance Frameworks / Karla McKenna
Link to presentation https://cloud.gleif.org/s/PLRAXDXmttXinkJ

Presented the components and experience creating the Ecosystem Governance Framework for the verifiable LEI (vLEI) by GLEIF (Global Legal Entity Identifier Foundation) based on the Trust over IP framework metamodel.

1. Introduction to Ecosystem Governance & Identity

- The **Trust over IP (ToIP) Meta Model** provides a governance framework for managing digital trust ecosystems.
- The ecosystem governance framework (EGF) is a **living document**, updated annually, ensuring relevance, security, and clarity in managing organizational identity.
- Focuses on **digitizing the Legal Entity Identifier (LEI)** to create **verifiable organizational identity**.

2. Evolution of the Governance Framework

- First framework launched in **2022**, with periodic updates.
- The **second-generation model** integrates learnings from previous versions.
- Governance **ensures trust** through an annual review process.

3. Verifiable Legal Entity Identifiers (VLEI)

- The **VLEI digitizes the LEI**, providing an **organization-level verifiable credential**.
- Issued by **qualified VLEI issuers**, ensuring **trust and security**.
- Acts as an **E-Seal equivalent**, enabling **secure digital transactions**.

4. Framework Interoperability & Reference to Other Standards

- The governance framework **aligns with other digital identity standards** (e.g., UK's digital identity framework).
- It **references external regulatory updates** but maintains flexibility for different implementations.

5. Credential Issuance & Trust Model

- Root of trust established through **a verifiable issuance process**.
- Two levels of credentials:
  - **Official credentials** (e.g., CEO, board members).
  - **Functional credentials** (e.g., employees, operational roles).
- **Credentials are chained**: individuals' verifiable credentials link to organizations, ensuring a **hierarchical delegation of authority**.

6. Decentralization & Hybrid Model

- **Hybrid model**: Centralized root of trust, **decentralized verification**.
- Ledgers, receipts, and signatures used to record **issuance, revocation, and key rotations**.
- **Automated verification** minimizes human intervention.

7. Challenges in Governance & Compliance

- **Trust & enforceability**: Governance framework must balance **technical automation** with **legal compliance**.
- Smart contracts pose **legal complexities** (e.g., proving user understanding of agreements).
- Need for **continuous verification & monitoring** to ensure **credential validity**.

8. Application of Verifiable Organizational Identity

- Used across sectors: **HR onboarding, financial compliance, copyright & royalties**.
- Example: Music industry—credentials ensure that royalties flow **directly to the rightful owners**.
- VLEI as a **modular identity component**, adaptable to different applications.

9. Barriers to Adoption in Africa

- **Legal entity verification is costly and complex** in some regions.
- **Limited adoption of LEIs** outside of large corporations.
- Strategies to **democratize access**, including integration with **business registries**.

10. Trust Framework & Relying Parties

- Trust ecosystem involves **issuers, verifiers, and relying parties**.
- Example: Secure Citizen **issues and verifies credentials** within a closed system, but broader adoption requires **governance trust**.
- Governance as **code**: Policies should be **automatable** but also **human-auditable**.

11. Future Considerations

- **Governance frameworks should be modular**, allowing gradual complexity.
- **Defining liability and accountability** in decentralized ecosystems.
- **Legal frameworks must evolve** to support automated governance models.

12. Key Takeaways

- **Governance is crucial** for **trusted digital identity ecosystems**.
- **Hybrid decentralized models** allow trust to be distributed without losing control.
- **Clear delegation of authority** enables efficient **role-based access** within organizations.
- **Africa's digital identity landscape** needs tailored solutions for **scalability and accessibility**.

SESSION #2

Session 2A

What makes up a Corp ID / Biz ID? ? LEI is one part - what other parts should be considered? And Organizational Identity (LEI and vLEI)

Session Convener: Cindy and Karla
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Notes for Organizational Identity (LEI and vLEI) - Karla

Background on identification of organizations using the LEI made verifiable by the verifiable LEI (vLEI)

Link to presentation: https://cloud.gleif.org/s/NAnwG4LkesZPfpJ

Session 2C

How to navigate implementation complexities for an inclusive digital ID to ensure NO ONE IS LEFT BEHIND

Session Convener: Sarah Mulaji
Session Notes Taker: **Thokozile Mcopele (TK) (Ms)**

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Key Topics:

- **Digital Wallets and Verifiable Credentials:** the concept of digital wallets and verifiable credentials, explaining how they work and their importance in the context of decentralized technology. Emphasized the need for a transition period for people to understand and adopt this technology.
- **Custodial vs Non-Custodial Wallets:** the difference between custodial and non-custodial wallets, highlighting the challenges faced in today's reality with moving technology to unfamiliar areas, especially in third-world countries like South Africa. Discussed the importance of education and the transition process for users to take custody of their wallets.
- **Web 2 vs Web 3:** shared an overview of the evolution of the internet from Web 1 to Web 3, explaining the fundamental differences and the importance of verifiable credentials in Web 3. Emphasized the need for control over personal information and the role of technology in achieving this.
- **Digital Identity for Rural Areas:** discussed the challenges and potential solutions for creating digital identities for people in rural areas. Emphasized the importance of infrastructure, education, and trust in implementing digital identity solutions.
- **Inclusivity and Accessibility:** discussed the importance of inclusivity and accessibility in digital identity solutions. Highlighted the need to consider different channels, such as USSD, SMS, and offline options, to ensure that everyone can access digital services.
- **Role of Chiefs and Community Leaders:** explored the role of chiefs and community leaders in verifying identities in rural areas. Discussed the potential challenges and benefits of involving local leaders in the process.
- **Education and Trust:** emphasized the importance of education and trust in implementing digital identity solutions. Discussed the need to educate people about digital identities and build trust in the system to ensure successful adoption.
- **Practical Examples and Use Cases:** shared practical examples and use cases of digital identity solutions in rural areas. Discussed the importance of addressing real-life challenges and learning from existing implementations.

Main ideas we discussed:
Digital Wallets

- Using custodial wallets to manage digital identities for users who are not yet familiar with decentralized technology
- Transitioning from custodial to non-custodial wallets as users become more familiar with the technology
- Explaining digital wallets in simple terms to ensure understanding among all users
- Using digital wallets to interact with verifiable credentials and blockchain technology
- Implementing digital wallets as mobile applications for easy access and interaction

Web Evolution

- Understanding the transition from Web 1.0 to Web 3.0 and its implications for digital identity
- Highlighting the importance of privacy and control in Web 3.0
- Exploring the role of verifiable credentials in Web 3.0
- Addressing the challenges of transitioning from Web 2.0 to Web 3.0
- Emphasizing the need for user education in adopting Web 3.0 technologies

Inclusivity and Access

- Using USSD and SMS as alternative channels for digital identity interaction is limiting to verify identity
- Implementing QR codes for offline access to digital identities
- Leveraging existing community structures, such as chiefs or community leaders, for identity verification
- Providing digital identity services through existing applications used by disadvantaged communities
- Ensuring accessibility to digital identity services through various technological means

Rural and Underserved Communities

- Developing digital identity solutions that cater to the specific needs of rural and underserved communities
- Using digital identities to enable economic participation without requiring physical relocation
- Addressing the lack of infrastructure, such as internet connectivity, in rural areas
- Exploring the use of verifiable credentials for non-financial purposes, such as accessing healthcare services
- Educating rural communities about the benefits and uses of digital identities

Session 2D

Backup and Recovery in a truly Self-Sovereign and Decentralized World

Session Convener: Robbie Blaine
Session Notes Taker: Robbie Blaine

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Scenario:
We have achieved utopia. There's no such thing as a "Custodial Wallet." Every holder, issuer, verifier, etc manages their own credential wallet and keys in their own way.
In such a world, how do users backup and restore their wallets?

Firstly, there are two pieces of data that constitute an SSI Wallet:

- The keys (e.g: 12/16/24/etc word mnemonic)
- The raw Verifiable Credential (VC) data in a database (DB) (e.g: on device SQLite)

Backing up the keys is very easy - paper, hardware (e.g: Ledger, Trezor) - that's already solved.
The question is primarily around the actual VC data.
In Custodial solutions, the VC data is stored for every customer in a centralized database.
However, seeing as we've achieved utopia, this no longer exists.
The responsibility for the storage, backup, and recovery for this data lies with the users themselves.

The vast majority of users will gravitate to a solution that is easy to implement and that they already use on a daily basis. For these users, standard iCloud and Google Cloud backups will be the go to. It will be up to SSI Wallet developers to integrate and develop solutions.

Many wallet developers will cater to the majority of users and implement a simple "Backup to iCloud/Google Cloud" solution (similar to Whatsapp).
Some wallet providers will implement their own proprietary backup solutions where you pay a monthly fee and the wallet provider will handle backups for you. This regresses back into a more custodial approach.

And a niche of die-hard Self-Sovereign users will gravitate towards wallet applications that allow them to fully manage their own backup solution.

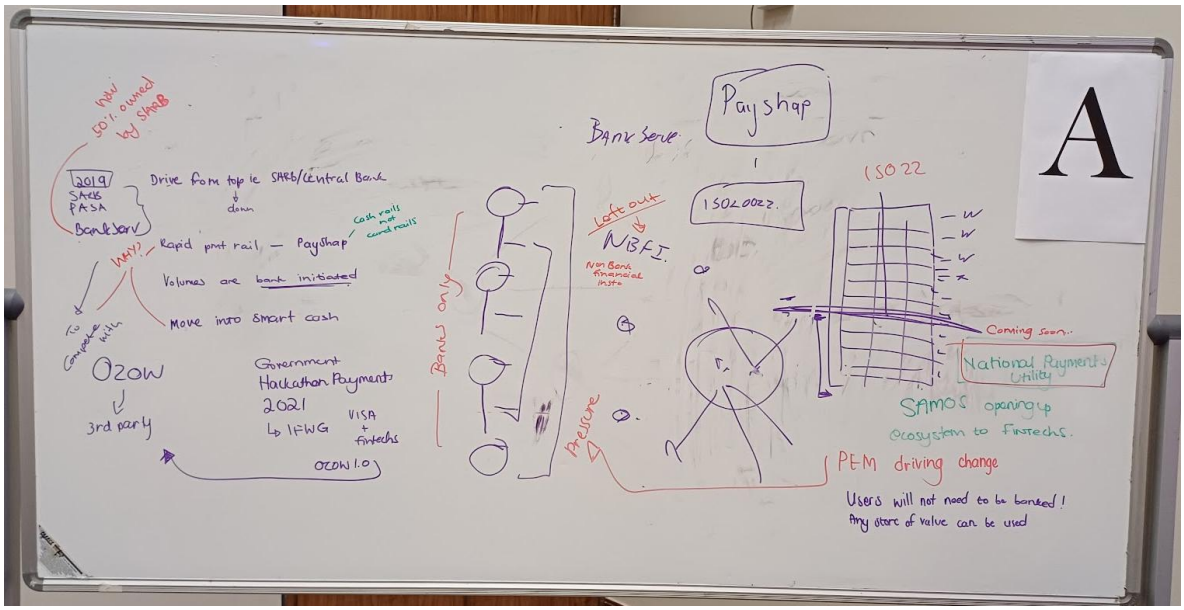
SESSION #3

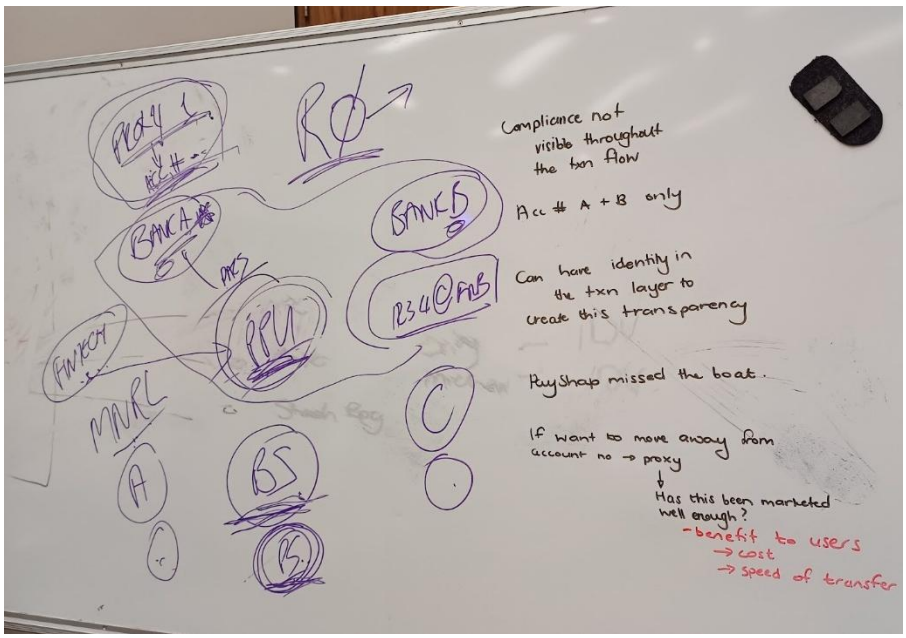
Session 3A

PAYSHAP: The Journey + where to next? combined with Financial Inclusion

Session Convener: Candice Mesk on Payshap, Lohan Spies on Financial Inclusion
Session Notes Taker: Candice Mesk

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?





Session 3C

How do we get Government on board?

Session Convener: Merryl Ford
Session Notes Taker: Merryl Ford

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

- Lots of press articles on SAfricans getting a digital ID
- How do we make sure that a centralised system is not developed? And is SSI ready for a country use case?
- If a different approach is used, is this a problem?
- Discussions
    - No, not a problem, there will be ways to integrate on a tech level
    - There would need to be a hybrid system anyway.
    - However, in terms of functionality, it will be a great shame, you won't be able to harness a lot of the value, e.g. sharing very specific fields in VCs.
    - Butan has a full SSI implementation
    - EIDAS v2 will also support a verifiable credential approach when it is rolled out
    - Idea: “Bring a government official to next year's conference”
    - Target City of Cape Town
    - Also it will take a long time to develop a national (DHA) citizen digital ID - need to roll out multiple use cases from the private sector that are non-threatening- start building an ecosystem to demonstrate how exactly it works. Avalanche of evidence and working systems that cannot be ignored.

SESSION #4

Session 4A

Authoring DI for "Dummies" - Adoption (industry agnostic, individual, juristic, regulators)

Session Convener: Dalene Deale
Session Notes Taker: Gideon Lombard

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

This session aims to establish a shared foundation for discussing the development and adoption of digital and decentralized identity (DI) technologies across diverse sectors, including individuals, businesses, and regulatory bodies. A key challenge in this space is the fragmentation of terminology and conceptual understanding, making it difficult to align on industry-wide standards, implementation strategies, and governance models. By defining a common language and point of departure, we can bridge the gap between technical experts, policymakers, and adopters, ensuring that digital identity solutions are interoperable, privacy-preserving, and accessible. Through this session, participants will gain clarity on the critical terms, frameworks, and principles shaping the DI ecosystem, fostering informed discussions that drive responsible and scalable adoption.

No.	Abbreviation	Description
1	ABIS	Automated Biometric Identification System
2	ACA	Attribute-based Access Control
3	ACF	Authentication Context Framework
4	AES	Advanced Electronic Signatures
5	AI	Artificial Intelligence
6	AML	Anti-Money Laundering
7	API	Application Programming Interface

8	AS	Authorization Server
9	AT	Access Token
10	ATP	Automated Transaction Processing
11	BBS+	Boneh-Boyen-Shacham Signature Scheme
12	BC	Blockchain
13	BCP	Blockchain-based Credential Presentation
14	CA	Certificate Authority
15	CASPs	Crypto Asset Service Providers
16	CBDCs	Central Bank Digital Currencies
17	CDD	Customer Due Diligence
18	CEN	European Committee for Standardization
19	CFTC	Commodity Futures Trading Commission
20	CIPC	Companies and Intellectual Property Commission
21	CIP	Customer Identification Program
22	CIAM	Customer Identity and Access Management
23	CII	Critical Infrastructure Information
24	CN	Common Name (in digital certificates)
25	COFI	Conduct of Financial Institutions Bill

26	CP	Certificate Policy
27	CRL	Certificate Revocation List
28	CSAM	Cybersecurity and Authentication Mechanisms
29	DCEP	Digital Currency Electronic Payment
30	DFID	Digital Financial Identity
31	DHA	Department of Home Affairs
32	DID	Decentralized Identifier
33	DIDS	Decentralized Identity Systems
34	DLT	Distributed Ledger Technology
35	DRM	Digital Rights Management
36	DS	Digital Signature
37	EBSI	European Blockchain Services Infrastructure
38	ECB	European Central Bank
39	ECT	Electronic Communications and Transactions
40	ECTA	Electronic Communications and Transactions Act
41	e-ID	Electronic Identification
42	e-KYC	Electronic Know Your Customer
43	e-Sign	Electronic Signature

44	EUDI	European Digital Identity
45	EU	European Union
46	FAPI	Financial-Grade API
47	FATF	Financial Action Task Force
48	FIDO	Fast Identity Online
49	FIDO2	Advanced Authentication Standard (Passkeys, WebAuthn, CTAP)
50	FIPS	Federal Information Processing Standards
51	FSCA	Financial Sector Conduct Authority
52	GDPR	General Data Protection Regulation
53	GLEIF	Global Legal Entity Identifier Foundation
54	HANIS	Home Affairs National Identification System
55	HSM	Hardware Security Module
56	IAL	Identity Assurance Level
57	ID&V	Identification and Verification
58	IEC	International Electrotechnical Commission
59	ISO	International Organization for Standardization
60	IoT	Internet of Things
61	IPFS	InterPlanetary File System

62	ISS	Issuer (Credential Issuer)
63	ITU	International Telecommunication Union
64	JWT	JSON Web Token
65	KBA	Knowledge-Based Authentication
66	KYC	Know Your Customer
67	LACChain	Latin America & Caribbean Blockchain Network
68	LEI	Legal Entity Identifier
69	LSP	Ledger Service Provider
70	MFA	Multi-Factor Authentication
71	MNO	Mobile Network Operator
72	mTLS	Mutual Transport Layer Security
73	MVP	Minimum Viable Product
74	NCR	National Credit Regulator
75	NDI	National Digital Identity
76	NFC	Near Field Communication
77	NIN	National Identification Number
78	NIST	National Institute of Standards and Technology
79	NIX	Non-Interactive Zero-Knowledge Proof

80	NPS	National Payment System
81	OIDC	OpenID Connect
82	OIML	International Organization of Legal Metrology
83	OTP	One-Time Password
84	PA	Prudential Authority
85	PACS	Payment Clearing and Settlement
86	PASA	Payments Association of South Africa
87	PAIN	Payment Initiation
88	PCTF	Pan-Canadian Trust Framework
89	PEM	Payment Ecosystem Modernisation
90	PEP	Politically Exposed Person
91	PID	Person Identification Data
92	PKI	Public Key Infrastructure
93	PoC	Proof of Concept
94	POPIA	Protection of Personal Information Act
95	PoS	Point of Sale
96	PP	Privacy Policy
97	PPU	Public Payments Utility

98	PSPs	Payment Service Providers
99	PWD	Password
100	QES	Qualified Electronic Signatures
101	QKD	Quantum Key Distribution
102	QTSPs	Qualified Trust Service Providers
103	RBAC	Role-Based Access Control
104	RBA	Risk-Based Authentication
105	RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act
106	RTC	Real-Time Clearing
107	SADC	Southern African Development Community
108	SAFBC	South African Financial Blockchain Consortium
109	SAMOS	South African Multiple Option Settlement
110	SARB	South African Reserve Bank
111	SARS	South African Revenue Services
112	SBTs	Soulbound Tokens
113	SC	Smart Contract
114	SGD	Digital Singapore Dollar
115	SIM	Subscriber Identity Module

116	SMS	Short Message Service
117	SSI	Self-Sovereign Identity
118	SSN	Social Security Number
119	SSO	Single Sign-On
120	TCIB	Transactions Cleared on an Immediate Basis
121	TEE	Trusted Execution Environment
122	TSP	Trust Service Provider
123	UBI	Universal Basic Income
124	UIDAI	Unique Identification Authority of India
125	UK	United Kingdom
126	US	United States
127	USSD	Unstructured Supplementary Service Data
128	VCs	Verifiable Credentials
129	vLEI	Verifiable Legal Entity Identifier
130	VDR	Verifiable Data Registry
131	VC-JWT	Verifiable Credential using JSON Web Token
132	VC-ZKP	Verifiable Credential using Zero-Knowledge Proofs
133	W3C	World Wide Web Consortium

134	WCAG	Web Content Accessibility Guidelines
135	WOT	Web of Trust
136	ZKP	Zero-Knowledge Proof

Session 4 D

Who has case studies? Let's hear them!

Session Convener: Fraser Edwards
Session Notes Taker: Fraser Edwards

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Focus was on any implementations of SSI / DID which are referenceable, ideally including a client. There will be a DID map published soon.

Vendor / supplier	Client	Use-case	State	SSI / DID / Credentials
Umazi	Isle of Man	Corporate identity	Pilot	Yes
Dock	Classter	Education	?	Yes
Dock	Port of bridgetown	Workforce management?	?	Yes
Dock	Daon	reusable identity	?	Yes
Dock	Socure	reusable identity	?	Yes
DIDx	Yoma	Education	Prod	Yes
DIDx / Secure Citizen	Twytch	rKYC - ridehailing	Development	Yes
Nymlab	Italian professional registry	eSignature?	Prod	Yes
eSatus	Ingo	Workforce management - construction	Prod	Yes
Truu	UK National Health Service	Workforce management - health	?	Yes
?	Jo'burg university	Education	Prod	No
Vera	?	KYB	Development	Yes
Proofspace	Cardano	Proof of attendance	?	Yes

Proofspace	Japanese project?	?	?	Yes
PRISM / Identus	?	?	?	Yes
LinkedIn	LinkedIn	Workforce management	Prod	Yes
GravID	?	?	?	Yes
GLEIF	?	Workforce management	?	Yes
GLEIF	?	IP management - music	?	Yes
Provenant	?	Call authentication	?	Yes
GLEIF	?	Trade Finance x 2	?	Yes
GLEIF	?	Digital product passports x 2	?	Yes
GLEIF	?	Pharmaceuticals?	?	Yes
PRISM / Identus	NZ Tribes	Identity	?	Yes
2060.io	?	?	?	Yes
Profila	Profila	?	?	?

SESSION #5

Session 5C

SA: Who isn't here but should be?

Session Convener: Fraser Edwards
Session Notes Taker: Fraser Edwards

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Original intention was to discuss SA SSI / DID builders that weren't present at the unconf, but since it seemed everyone building SSI / DID was already here, ended up focusing on who we would want to attend in general, especially next time:

- Banks
- Universities
- Google, Apple, Microsoft
- Consulting firms:
    - PwC
    - Accenture
    - KPMG
- Other global implementers, e.g. from Ayra / GAN
    - Possibly do a structured day with some virtual presentations to get opinions in from outside
    - E.g. Quandata
- Retail ecosystems:
    - e.g. Take-a-lot, the Foschini group, The Bulk Market,
- More technical people:
    - Architects
    - BC Gov
    - Universities
    - Digital ID researcher
    - *Need to find them*
- Deliveries
- Government - bring a government official to work day
    - City of cape town
- Next year, take a list of the use-cases and case studies to entice government and industry to attend

Anushka Soma-Patel • 1st

Innovator. Keynote Speaker. Educator. Collaborator. Independent Co...

2mo •

Wow! What a wonderful day 2 of did:unconf from sunrise to sunset and beyond! We discussed topics crafted by participants that enabled us to understand the available tech and use cases as well as the next potential use case/s with known and new connections within the open spaces enabled by the unconference workshop format!

It's been an invaluable day of amazing conversations and connecting! Thanks DIDx , Heidi Nobantu Saul , Fraser Edwards , Carrie Peter , Lohan Spies , Gideon Lombard , Tina Valab , Merryl Ford and many others who I have not hear connected with on LinkedIn

Session Notes / Thursday February 20 / Sessions 6 - 10

SESSION #6

Session 6A

The Role of Integrated Identity Platforms in the creation of DFIDs. Are they bound to one another?

Session Convener: Jason Shedden
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

No Notes Submitted

SESSION #7

Session 7F

Preventing 1984

Session Convener: Willem Basson
Session Notes Taker: Robbie Blaine

The scene:
We have a system where your financial transactions are directly linked to your identity.
If I want to buy a goldfish, in this system, my ID would be linked directly to that transaction.

Currently, we have cash to fall back on. But, if there were to be a hypothetical event that causes safety concerns of something that is transmitted via contact, cash could be banned/outlawed, and now we can only transact digitally with identity verification on all transactions.

Examples of risks:

- Donating to a rival political party.
- Donating to something that is, or could be, a controversial cause (abortion clinics, abuse shelters, homosexual charities).
- Purchasing something that is legal today, but is outlawed by a future government party.
- Dissenting against the state.

Real-world cases:
In 2022, in Canada, there was a trucker protest against vaccine mandates.
Many Canadians who donated money to support the protesting truckers had their bank accounts frozen. This prevented them from conducting any financial transactions. Even those who used Bitcoin didn't escape, as the funds were traced to Centralized Exchanges (Coinbase and Crypto.com), and their accounts were also frozen. (source).
More about Bitcoin's fungibility problems can be found here.

The United Kingdom Government has pressured Apple into disabling Advanced End-To-End Encryption for Apple iCloud Backups after trying to pressure them into adding a backdoor (source).

How do we prevent this from happening?
How do we embrace SSI, DID, DFID, etc while still maintaining strong privacy protections?
How do we build a censorship resistant system?
Some notes:

Privacy/anonymity should be **on** (opt-out) by default.
Users should be able to consent to be de-anonymized on an as needed basis.
People need to be educated about the importance of privacy.

Create something like a Spotify Wrapped where you can import your data from a website (e.g: Instagram) and then “Track the Tracker” analyzes it and gives you a “Spotify Wrapped” type view of all the places Instagram shared your data with.

Today, privacy and convenience is mutually exclusive.
How can we make it convenient to be private?

Centralized Digital Identity (CDID) is a significant problem.
A potential solution could be *Decentralized* Identity (DID).
Maybe we can, in our marketing, purposefully and consciously separate *Centralized* Digital Identity from *Decentralized* Identity.

I don’t need privacy, I have nothing to hide.
I don’t need freedom of speech, I have nothing to say.

SESSION #8

Session 8B

Standards? Reuse? Redo for Africa? & The future of OID4VC & DIDComm

Session Convener: Shaveen Bageloo and Max Coleman
Session Notes Taker: Max Coleman

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Key Discussion Points

1. DIDComm vs. OID4VC

- Both DIDComm and OID4VC enable the sharing of Verifiable Credentials (VCs), but they serve different purposes and offer unique advantages.
- **DIDComm**
  - Enables secure, encrypted communication between two DID holders (encrypted both at rest and in transit).
  - More than just verification, it supports peer-to-peer messaging and broader decentralized applications.
  - Platform-agnostic due to its transport-layer agnostic protocols, allowing interoperability between different messaging platforms.
  - Used by Bhutan's National Digital Identity (NDI) project.
  - Open question: Is it needed at this stage of development in Africa?
- **OID4VC**
  - Easier to adopt, particularly for enterprises and governments.
  - Built on top of OAuth, making it familiar to existing digital identity frameworks.
  - Recognized as the default for standards such as eIDAS in Europe.
- The general belief is that OID4VC is currently being utilized simply because it is easier to adopt. However, DIDComm enables much more - while the sharing of VCs creates a root of trust, DIDComm facilitates ongoing communications, document sharing, and further decentralized applications once trust has been established.

2. Africa's Approach to Decentralized Identity: Following EU Standards or Creating Its Own?

- **Current Landscape**
  - Africa faces significant inefficiencies in digital infrastructure and identity management.
  - European standards, such as eIDAS, have been designed specifically for Europe's needs.
  - South Africa's approach to GDPR serves as a precedent: instead of adopting it wholesale, South Africa created its own version, POPIA, to suit its unique regulatory environment.
- **Arguments Against Direct Adoption of EU Standards**
  - Europe has advanced technological capabilities, while only two African nations have comparable infrastructure.
  - Africa needs to play a role in shaping its own identity standards rather than passively adopting external frameworks.
- **Potential Benefits of DIDComm for Africa**
  - DIDComm's transport-layer agnostic nature allows VCs to be shared via text message, making it accessible to lower LSM groups.

- More adaptable to Africa's existing communication infrastructure, where mobile-based services are prevalent.

3. Decentralized Identity and Human Rights in Africa

- African governments will emphasize the **why** behind decentralized identity adoption, focusing on:
  - **Convenience:** Simplifying access to government services.
  - **NGO Enablement:** Supporting humanitarian efforts by providing secure and verifiable identities.
  - **Human-Centric Approach:** Ensuring that technology serves people's needs, particularly in underprivileged communities.

Conclusion

- Africa should leverage lessons from European standards like eIDAS while ensuring that its approach reflects its unique challenges and opportunities.
- OID4VC's simplicity makes it attractive for governments and enterprises, while DIDComm's flexibility and resilience make it well-suited for Africa's diverse technological landscape.

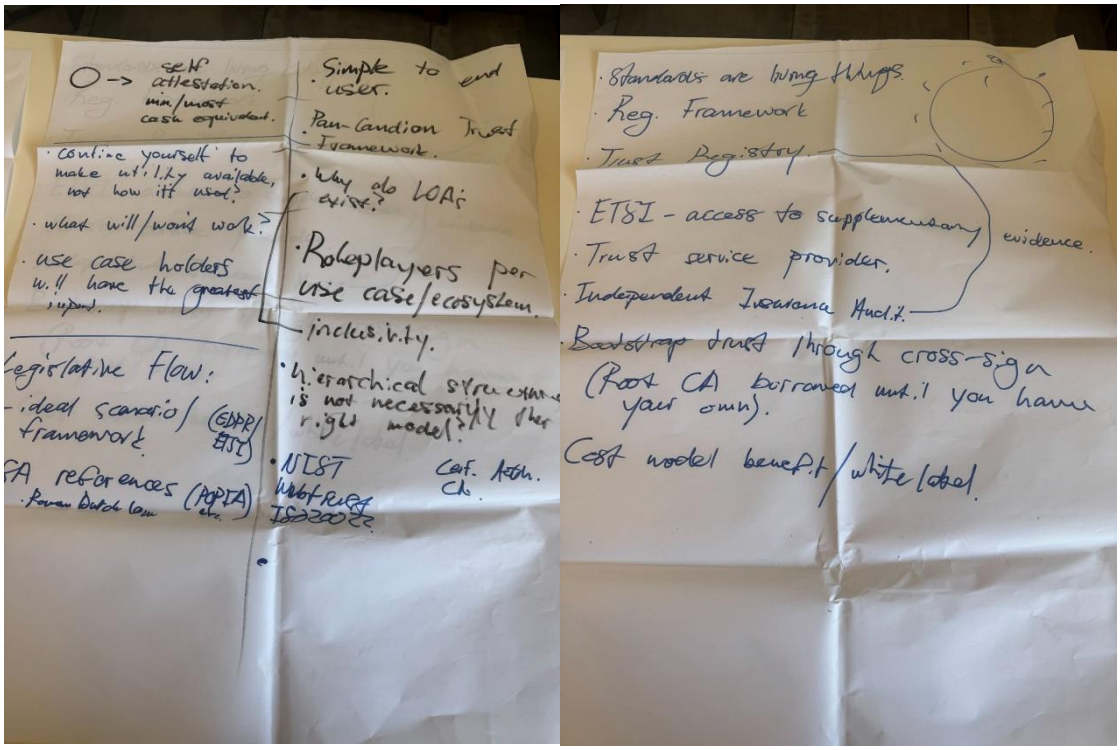
- A hybrid model that integrates components from both standards may offer the best path forward.

Session 8E

Levels of Assurance

Session Convener: Gideon L
Session Notes Taker: Gideon Lombard

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?



1. NIST Identity Guidelines (SP 800-63) – Levels of Assurance

The **National Institute of Standards and Technology (NIST) Special Publication 800-63** defines Levels of Assurance under **three key components**:

1.1 Identity Assurance Level (IAL) – Strength of Identity Proofing

- **IAL1**: Self-asserted identity, minimal proofing (e.g., email sign-up).
- **IAL2**: Remote or in-person proofing with validated documents (e.g., passport, ID verification).
- **IAL3**: In-person proofing with stringent checks, biometrics, and verified identity documents.

1.2 Authentication Assurance Level (AAL) – Strength of Authentication

- **AAL1**: Single-factor authentication (password, PIN, or OTP).

- **AAL2**: Multi-factor authentication (MFA) with at least two factors.
- **AAL3**: MFA with a hardware-based authenticator (e.g., cryptographic token, biometric device).

1.3 Federation Assurance Level (FAL) – Strength of Federation & Assertions

- **FAL1**: Basic assertion security (signed assertions).
- **FAL2**: Additional proofing, encrypted assertions.
- **FAL3**: Highest assurance, signed and encrypted assertions with identity binding.

2. ETSI (European Telecommunications Standards Institute) eIDAS Assurance Levels

ETSI aligns with the **EU's eIDAS Regulation** and defines **four levels**:2.1 ETSI Identity Assurance Levels (LoA)

- **LoA Low**: Self-declared identity, minimal proofing, weak authentication (similar to NIST IAL1/AAL1).
- **LoA Substantial**: Verified identity with document proofing, strong authentication (akin to NIST IAL2/AAL2).
- **LoA High**: Stringent identity proofing (in-person with biometric verification), cryptographic authentication (similar to NIST IAL3/AAL3).
- **Qualified Trust Services (QTS)**: Beyond **LoA High**, it applies **qualified electronic signatures** (eIDAS-compliant legal standing).

Key Differentiator: ETSI integrates **legal trust services** (e.g., Qualified Electronic Signatures) under eIDAS, whereas NIST is more focused on security and technical assurance.

3. Trust over IP (ToIP) – Levels of Assurance

The **ToIP model** is more **ecosystem-based**, emphasizing decentralized identity trust through governance, technology, and policy layers.3.1 ToIP Levels of Assurance

1. **LoA 1: Self-asserted identity** – User claims identity without external validation.
2. **LoA 2: Peer or Community Validation** – Identity is endorsed by trusted network participants.
3. **LoA 3: Institutional Verification** – Identity verified by government, financial institutions, or regulated entities.
4. **LoA 4: Cryptographic & Biometrics Binding** – Strongest assurance, includes cryptographic verifiable credentials & biometrics, with decentralized governance validation.

Key Differentiator: ToIP emphasizes **trust frameworks** and **verifiable credentials** over traditional **identity proofing methods**.

Comparative Overview of LoA Across Frameworks

Framework	LoA 1 (Low)	LoA 2 (Moderate)	LoA 3 (High)	LoA 4 (Highest/Regulated)
NIST	Self-asserted (IAL1)	Remote Proofing (IAL2)	In-Person Proofing (IAL3)	Federated with Strongest Auth (FAL3)
ETSI/eIDAS	LoA Low	LoA Substantial	LoA High	Qualified Trust Services (QTS)
ToIP	Self-asserted	Peer Validation	Institutional Verification	Cryptographic & Biometrics Binding

- **NIST** is security-driven, emphasizing **proofing, authentication, and federation**.
- **ETSI/eIDAS** is legally driven, aligning with **trust services and qualified digital signatures**.
- **ToIP** is **decentralized**, prioritizing **self-sovereign identity and cryptographic trust models**.

Each framework serves different needs:

- **Government and enterprise-driven systems** lean on **NIST and ETSI/eIDAS**.
- **Decentralized identity ecosystems** favor **ToIP** due to its cryptographic and peer-based trust models.

SESSION #9

Session 9A

Delegated Authority & Attestation Attributes

Session Convener: Karla and Carrie
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

We covered the definition of various terms relevant to the environment in both a trust and SSI framework.

Relying parties - those who can trust the person/data presented to them by a trusted source
Subscribers/holders - those to whom the information relates or belongs
Verification - the process of checking that the information/person can be trusted
Role - The rights and roles assigned to a person, the representations ta person can make about themselves in a trusted framework
Consent & Explicit consent - permission or access granted to information or agreements by a person/subscriber/holder - explicit implies that they must be fully aware of the extent of the permission they are granting
Legitimate cause - means that the data accessor must have a valid reason to request/use data about a person/entity
Legal Entity - non natural person
Natural Person - living person
Attestation Attributes & Verifyable Credentails - information data points that a person may want or need to share about themselves
Trust Register - a list/register of trusted parties

We raised the question of what qualifies as verified? and explored some of the existing verification frameworks.

We discussed some of the standards and protocols that enable remote verification across the internet.

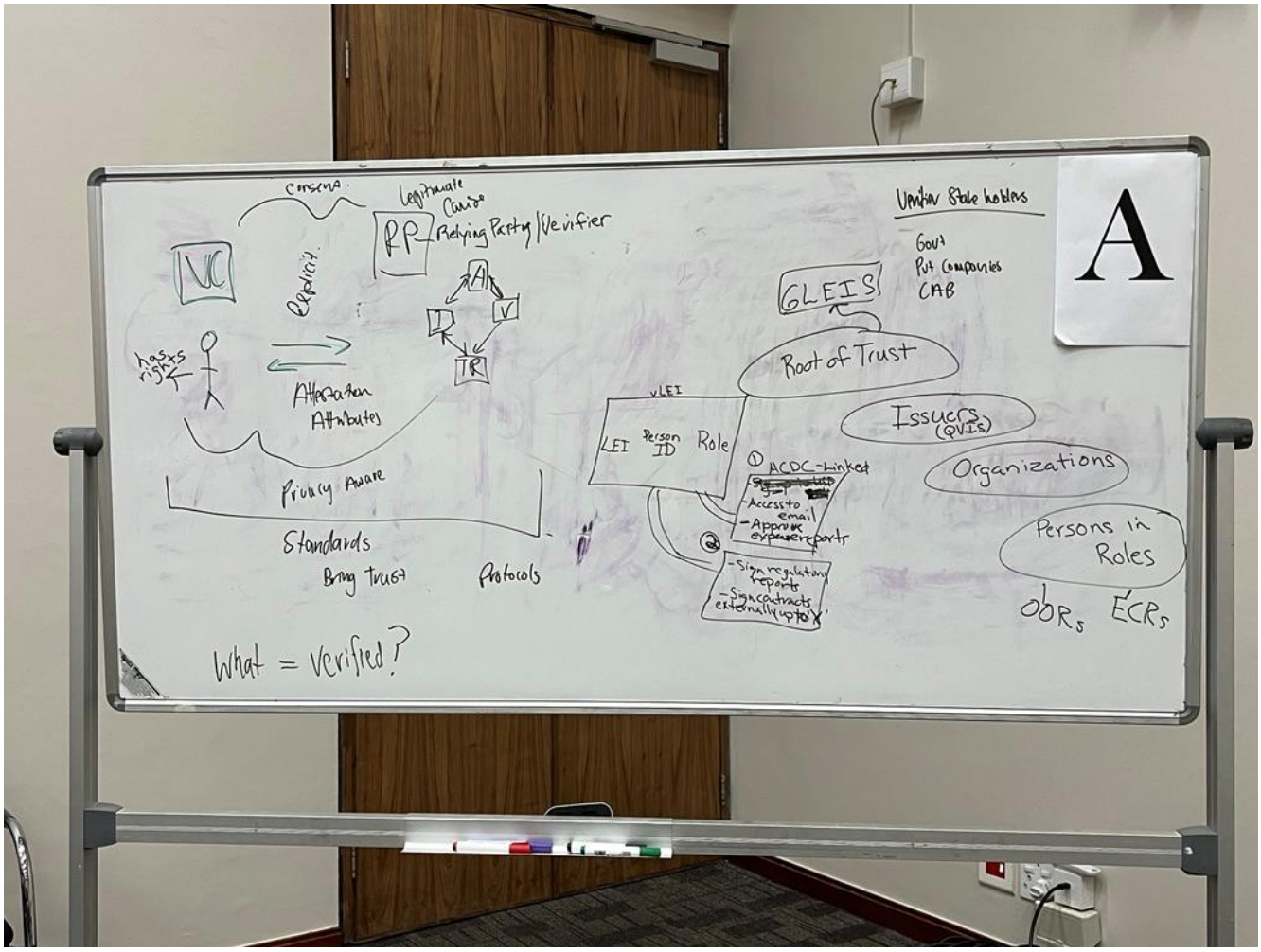
We identified the different types of stakeholders that may rely on verified information for various processes.

We then explored LEI's and the vLEI in detail.

1st we understood the process by which vLEI bestows company lined credentials to individual company representatives & how those can be verified back to the root credential.

2nd we discussed the current format of a vLEI.

3rd we discussed different use case examples of how vLEI's could be used within companies, and by external stakeholders.
Internally companies can use the credentials to grant access to systems, or networks, or to manage physical access.
Externally relying parties or verifiers can use the credentials to determine if they are interacting with the appropriate/appointed company representative.



Decentralized Smart Proxies

Session Convener: Lohan S
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

No Notes Submitted

SESSION #10

Session 10A

How to join the Twytch ecosystem? & Is the tech ready to demo and/or use?

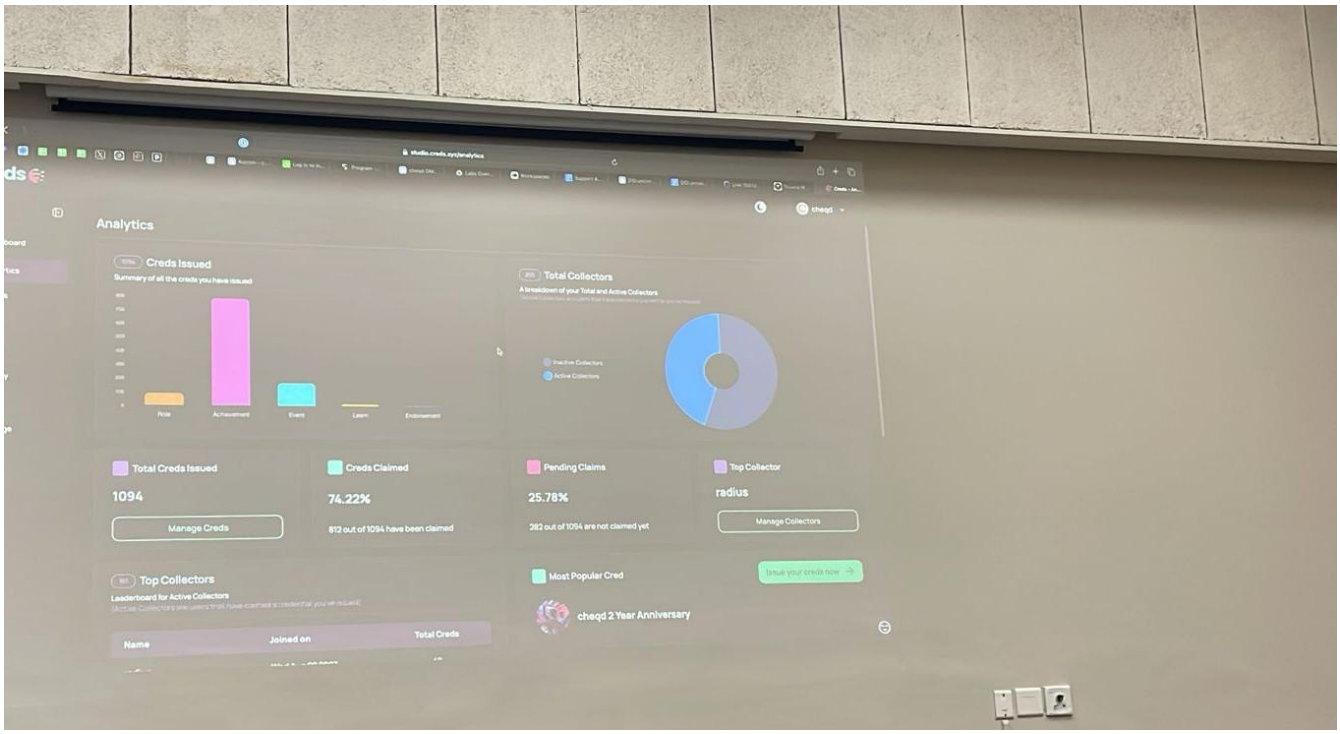
Session Convener: Anushka Soma-Patel
Session Notes Taker: Anushka Soma-Patel

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

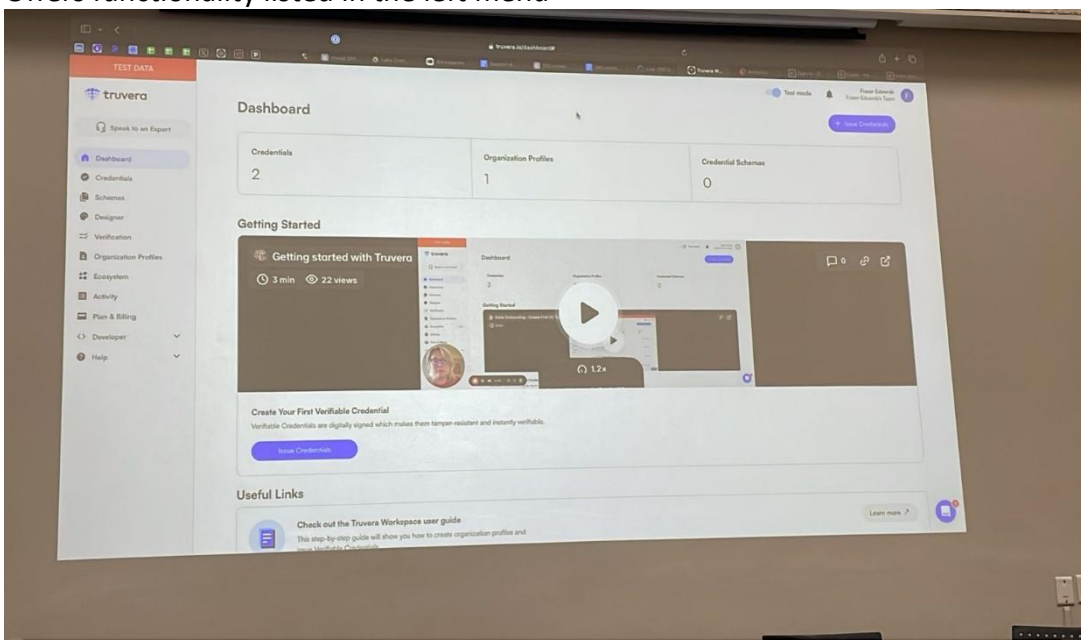
The demo session was great as it was an opportunity for people to see what we were talking about throughout the conference. This was particularly useful for people that are new to self sovereign identity, decentralised identifiers and verifiable credentials.

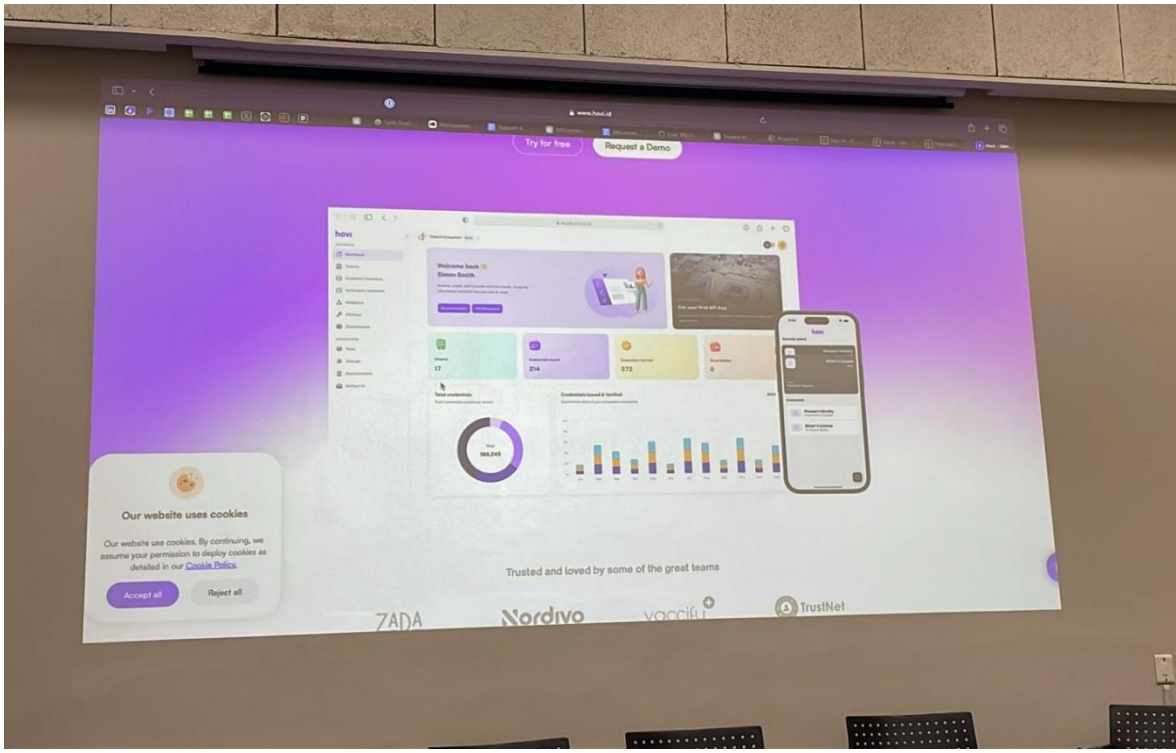
We had 4 presenters. note that my notes are not exhaustive and do not reflect all functionality in the system. Brief notes for each follow:

- Fraser
    - Demo: Cheqd credential issuance platform
        - Features:
        - Analytics dashboard for credentials issued

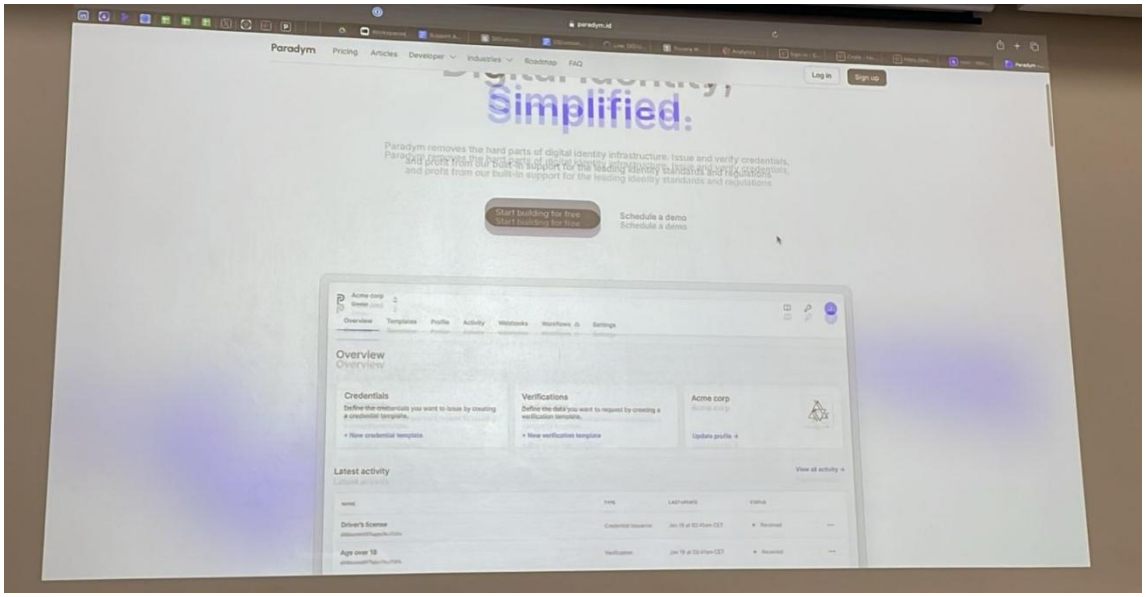


        - The holder can choose whether to accept a credential that was issued to them
        - Various types of credentials can be issued
        - Artwork can be added

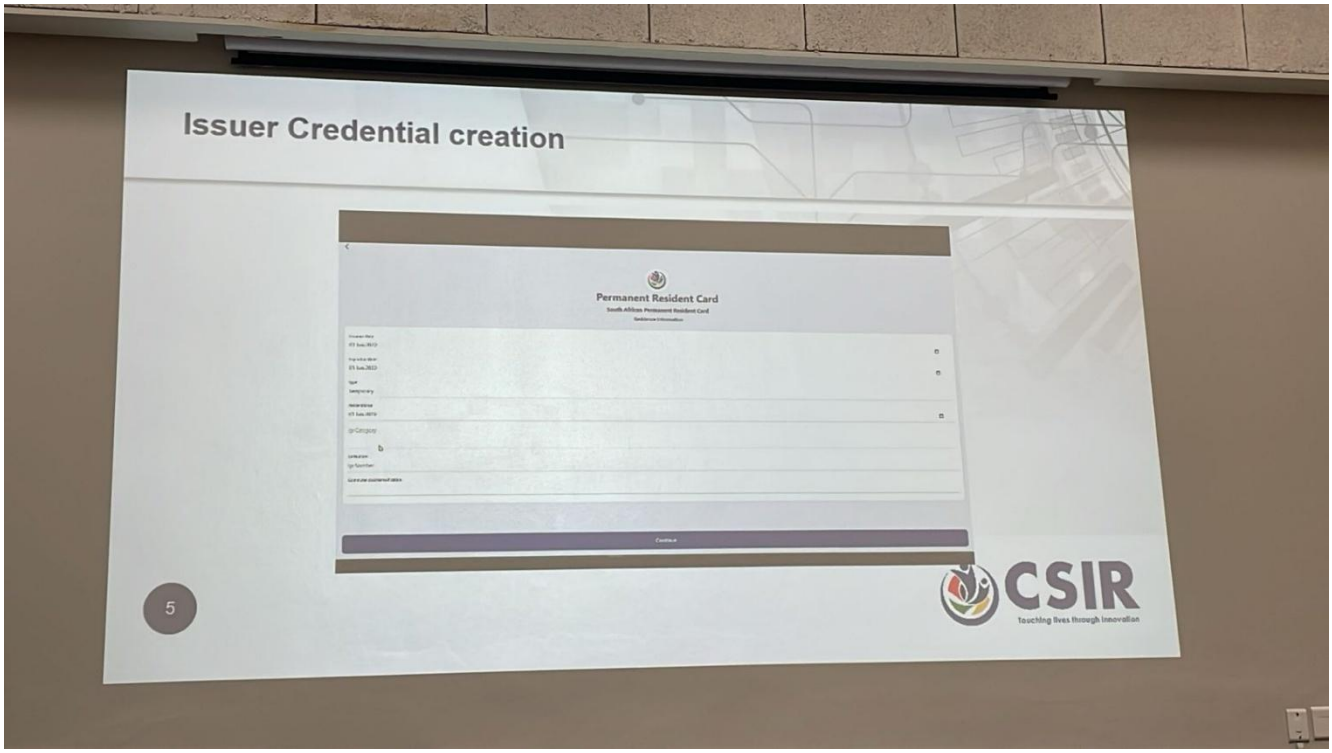
        - In future you could charge for the credential
        - Can issue to individuals or in bulk
        - Going to be used for gaming going forward
    - Demo: Docks platform
        - More generic platform
        - Offers functionality listed in the left menu
        - 

    - Demo: Hovi
        - is similar
        - 

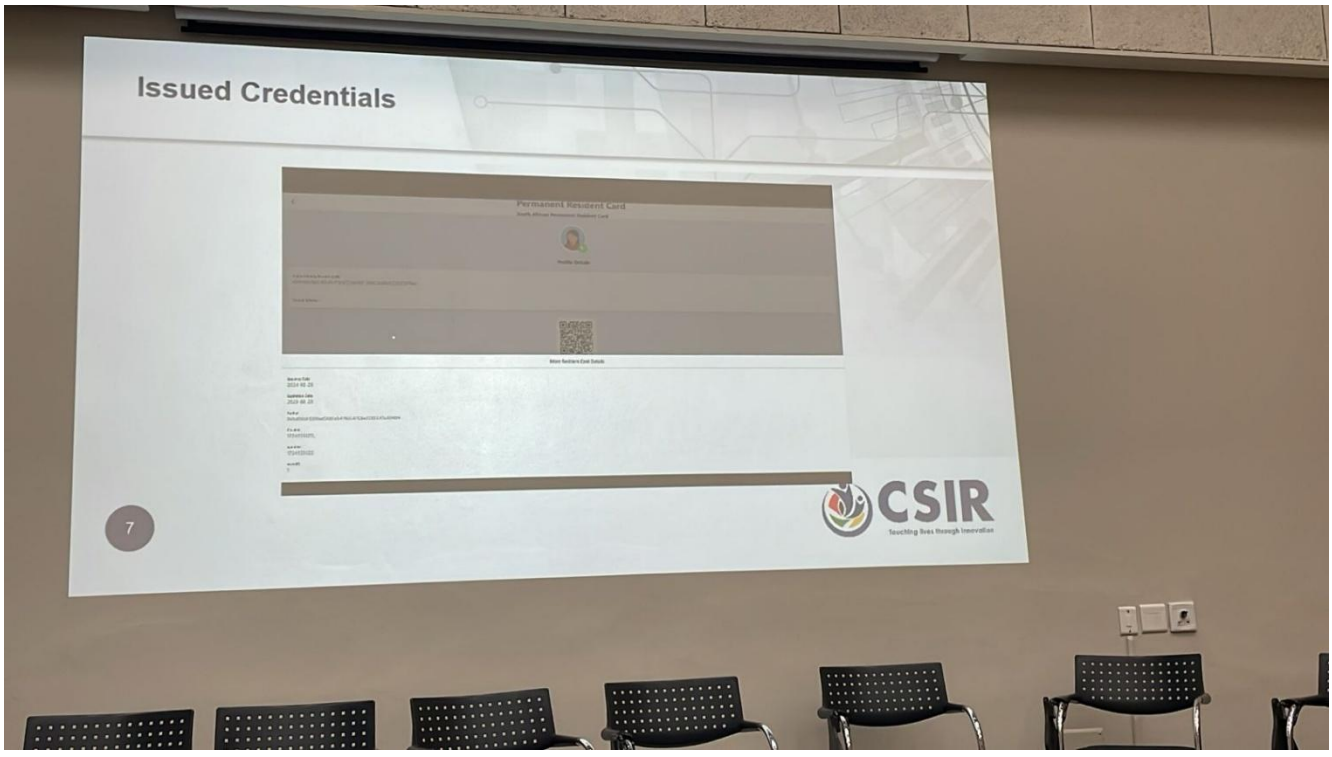
        - Demo: animo



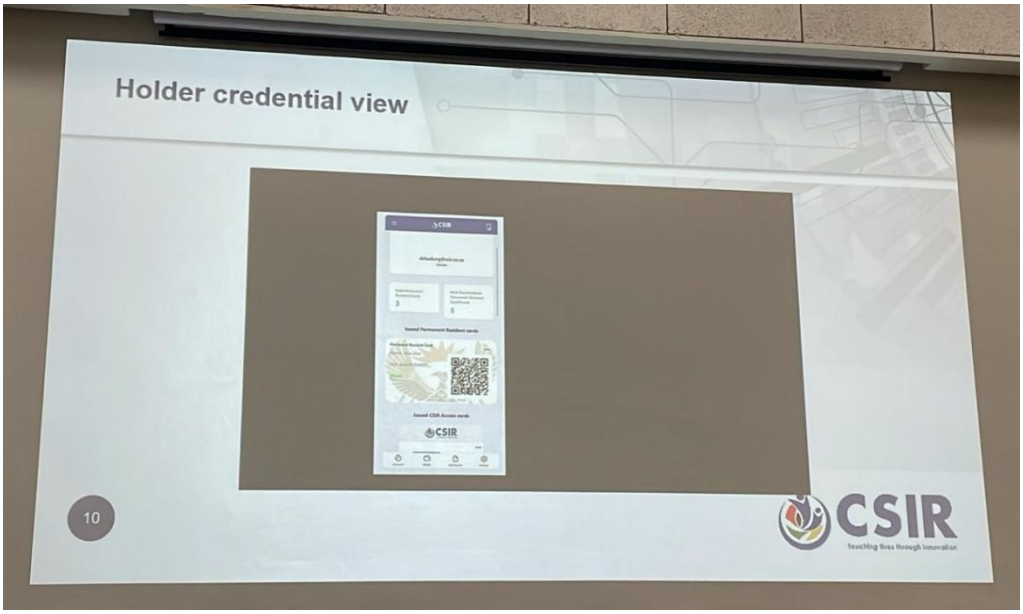
Presenter: Daniel from CSIR
Demo: CSIR visitor credential POC
Stage: development



- Using W3C standard
- issued credential:

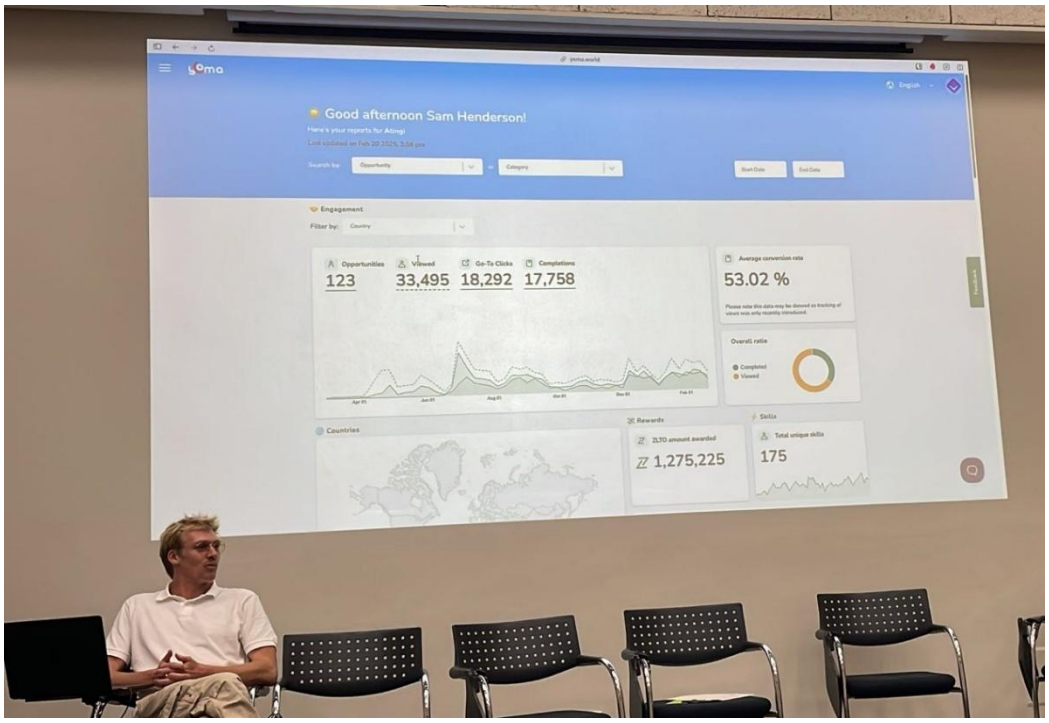


- - Web app holder wallet displaying issues credential

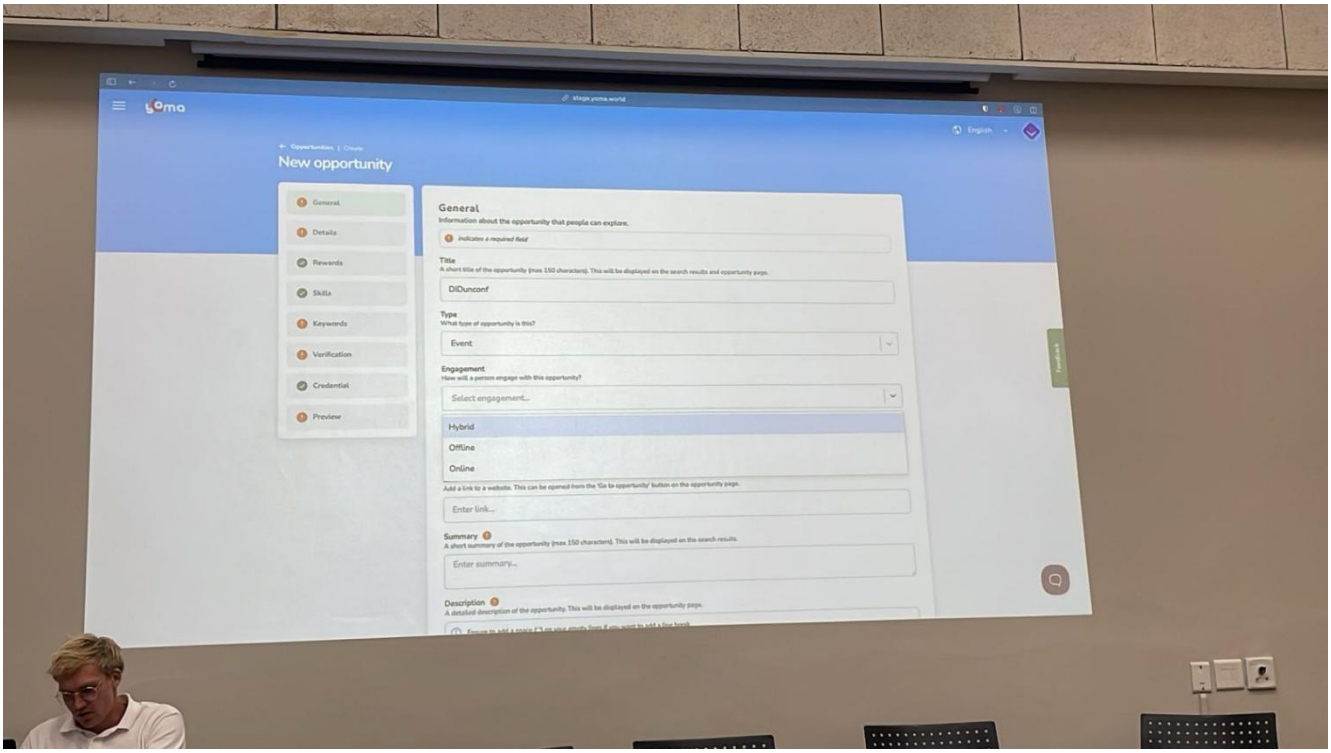


- Holder has ability to create a proof
- Allows selective disclosure
- In development. Going towards in house proof of concept
- Staff card issuance use case
- And access control fro visitors

Presenter: Sam
Demo: Yoma.world

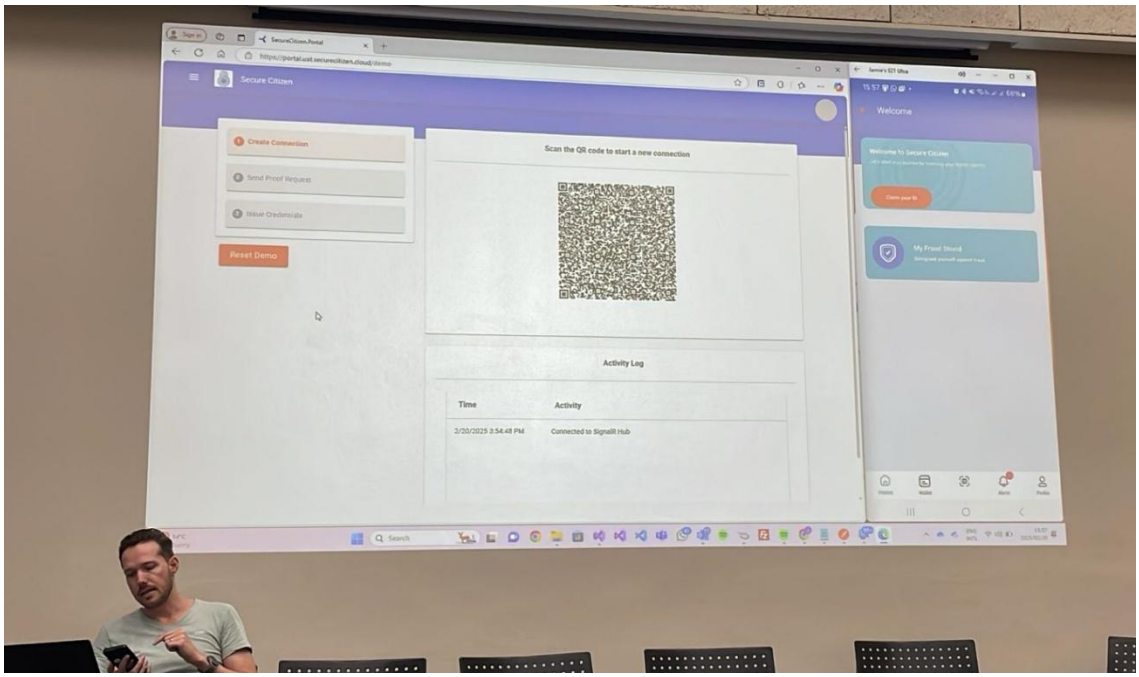


- Analytics dashboard
- Lots of data in the platform reflecting how many opportunities one worked on
- Setup a new opportunity



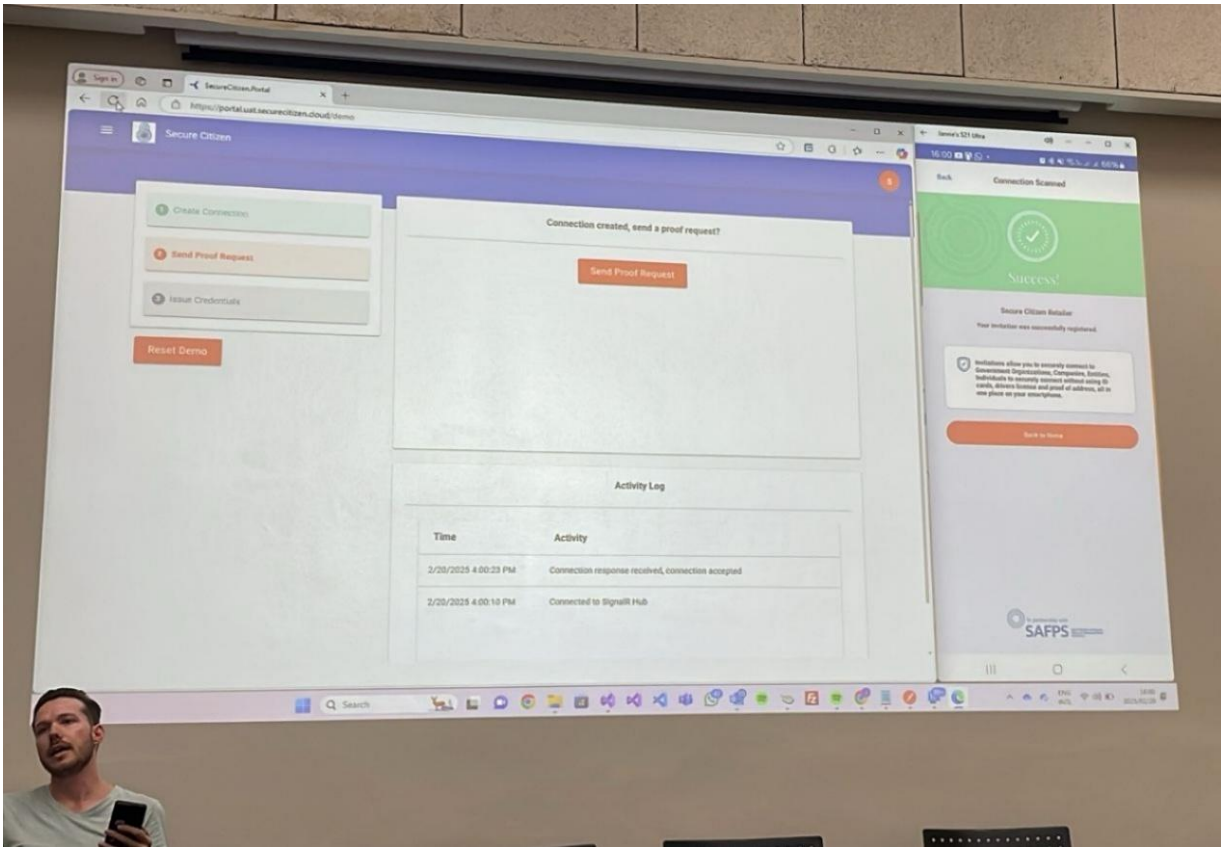
- Can issue zlato tokens to allow people to buy things from the market place
- Can create an opportunity and issue a qr code to track in person attendance

Presenter : Jannie
Demo: Secure citizen

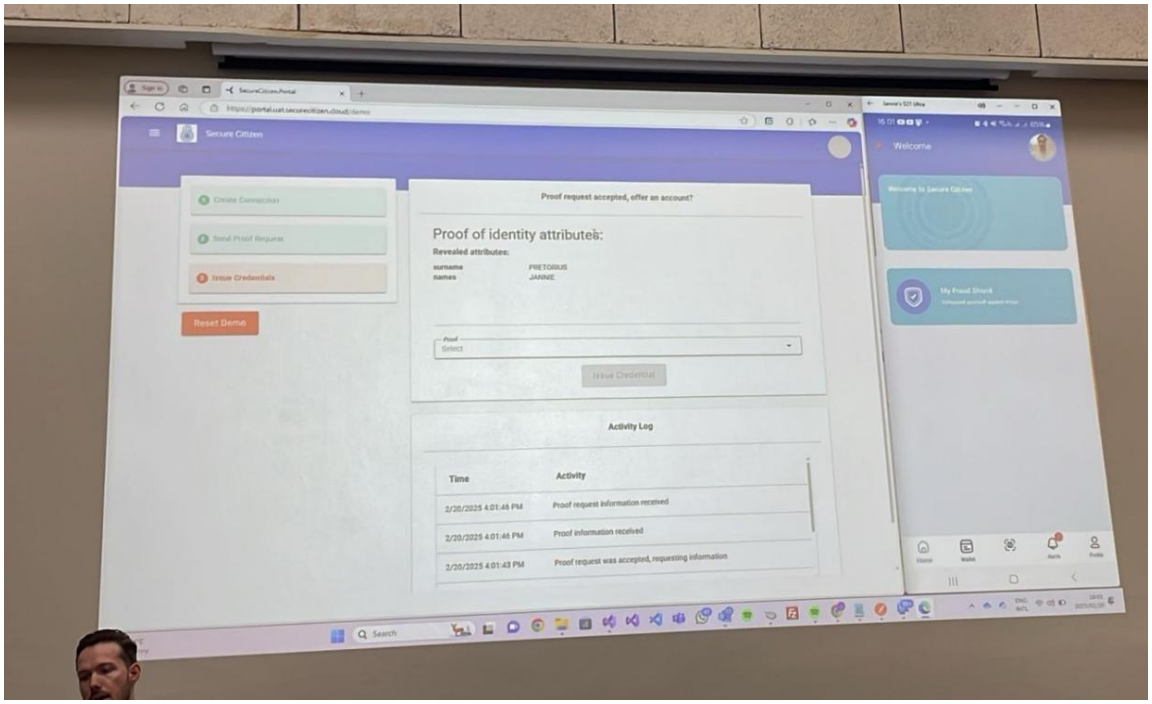


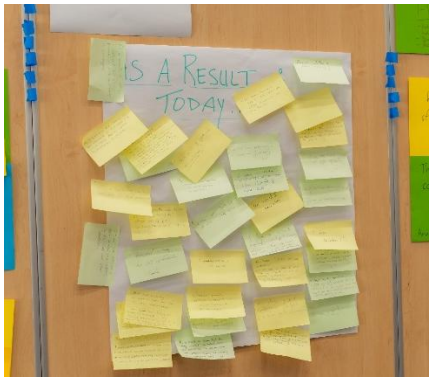
- Retail account opening use case
- Secure citizen
- Verifies ID against dha

- Proof of person credential
- Connect with retailer



- - Proof requested and shared by holder



Attendee Comments on Participating in DID:UNCONF AFRICA

Participants were asked to reflect on their first day of Open Space unConference and complete the sentence -

'As a result of today…'

I had the opportunity to attend multiple circles where innovative ideas were discussed. One of which was how to bridge the digital identity gap in a village without leaving anyone out, which also talks about Diversity and Inclusion.

I learned Patience

I am better informed and need to have lots more coffee to connect with new friends…

I understand better how the digitally illiterate will be taken into account while building digital identity. No one may be left behind!

Fewer slides —> More talking!

I realized that the passion in this community is contagious!

I am inspired

I had incredibly interesting insights regarding regulation within SA as well as the banking industry within the nation (and by extension where the opportunity persists.)

Fascinating - I learnt about PayShap and how its full potential is being hindered - Lohan's payment proxy talk was incredibly interesting too.

I feel excited!!!

SSI is closer than you think! & Jason will have a story to tell

I have a deep understanding of the issues faced by B2B concerns and the vast difference of B2C / voice of customer when receiving value from DID options.

Very interesting and knowledgeable people, both local and international

My "academic" spirit has been awakened. I'll be able to carry on from where I stopped in terms of writing my research. Very enlightening conversations.

I learned about PayShap; backup and recovery solutions; active use cases; and more! I did not learn enough about governance.

That the merge between decentralized identities and payment rail can potentially relieve both compliance burdens and preventing the greylisted status in SA

The 'Open Space Technology' method for conducting the conference was new to me and intriguing.

I have made new connections and learnt so much

I understand the value of DID can otter

I feel inspired and learnt a lot.

I know more about DFID and the PayShap exists.

I have a clear understanding of why this event is important!

I know what vc D&U are - Introduced to TWITCH + didX - Learned about PayShap - Found out about ISO-20022 - I am wiser 🤓

I learnt more about where PayShap had failed and how we can fix it

I have identified Gaps in my knowledge in the area of Digital Identities resulting in having a clearer mapping of what areas to focus on for further exploration of deep-dive

I made new, synergistic contacts! And learned about some really cool projects.

I have a little less fear of circle conversations! I have learnt that looking at solving (a) problem (s) is very inwardly focused - e.g. How do I perceive the problem as opposed to what is the actual pain point.

I have a greater appreciation of the complexity and various moving parts - I realized we're all figuring it out.

I know about so many more DID implementations + A's

I am more intrigued to follow modernization efforts by the SARB and other stakeholders

I have built a new network of DID enthusiasts

We identified potential collaborations for the next use case - We learnt of global and local use cases in various stages of implementation - We learnt what payshap is as its immediate settlement capability - We learnt who else should be in the room - at next years DID:UNCONF AFRICA - We made new contacts

I am reminded of the need for accessible and inclusive technology solutions

I realized learning is a constant journey

I see the value of (meeting using) Open Space!!

Thank you to our Scholarship Sponsor iiDENTIFii

At DID:UNCONF AFRICA, we are passionate about creating opportunities for students, emerging leaders, and individuals from marginalised communities to engage with the digital identity community. Our scholarship programme is designed to lower the barriers to entry for those who might otherwise be excluded—ensuring that young innovators and underrepresented voices from across Africa can participate, contribute, and help shape the conversations that matter.

Scholarships made it possible for four University of Cape Town students to attend and participate.

Online Posts by Attendees

Anushka Soma-Patel • 1st
Innovator. Keynote Speaker. Educator. Collaborator. Independent Consultant ...
1mo •

was even better than I imagined! Key take outs:

- **Shaun Strydom** and **Lohan Spies** explained the history and progress of digital identity, enabling people with zero knowledge of this subject to understand its importance and use in our daily lives (including the role of verifiable credentials and proof requests that enable a high level of trust in the Twych e-hailing ecosystem which will be launched this month.) 🙏

- digital identifiers enable us to 'do stuff' in our lives by enabling levels of trust between two parties. Globally, the **Ayra Association** is enabling trust between ecosystems. Being at the forefront of this tech wave is a very fulfilling experience which I will continue to share with my network 💖

- the open format of the unconference on day two and three enabled us to have very relevant conversations that ranged from explaining basic concepts to people new to the field, discussing the future that we may be enabling (good and bad), demo of the tech that enables the use of digital identity and digital identifiers as well as tech solutions for digital proxies etc etc. 🙌

- there are many next steps that will come from the discussion - so watch this space and I will definitely be sharing this info with my network 🤜

Lohan Spies, **Gideon Lombard** & **Heidi Nobantu Saul** thanks for creating this collaborative space for the trailblazers among us, I know that next year we will see some fast followers too 💖 🙏

Sarah M. • 2nd
PhD Candidate & Doctoral Research fellow
2mo • Edited •

My colleagues **Siyavuya Ntlale**, **Khairah Hoosen**, **Lablonde Juliette Kalalizi** and I attended the **DID:UNCONF AFRICA** 2025 from 18 to 20 February. This was the first in Africa and the only industry-oriented conference we have ever attended. I was marked by the warm welcome toward academia 😊

The topics discussed were interesting, relevant, innovative, and thought-provoking. I gained invaluable insights into the innovations happening locally and globally to make sense of my research around digital identity in South Africa.

It was inspiring to learn from different prominent voices in digital identity and Self-Sovereign Identity in Africa and from around the world, **Martin Grunewald**, **Anushka Soma-Patel**, **Merryl Ford**, Thokezile Mcopele, Lohan Spess, **Jason Shedden**, Kalra McKenna, to name a few.

I had the privilege to initiate a group discussion on "how to navigate complexities involved in implementing digital Identity solutions fit for the tAfrican context to ensure no one is left behind". We had a heated debate about the role of government and the impact of national digital identity, and self-sovereign identity on the most vulnerable in our society. We discussed ways to overcome the digital divide challenge for inclusive digital identity in Africa.

I thank **Gideon Lombard** and **DIDx** for sponsoring us. I am grateful to my supervisor, Prof. **Irwin B.**, for supporting me. Thank you to our Department of Information Systems for the invitation to represent UCT at this event. Looking forward to the **DID:UNCONF AFRICA** 2025 book of proceedings!

VERA
168 followers
1mo •

Reflections on DID:UNCONF AFRICA – A Defining Moment for Digital Identity in the SADC Region

Last week, the VERA team attended DID:UNCONF AFRICA which was unlike any other conference - no rigid agendas, no one-way keynotes. Instead, real, organic discussions unfolded, tackling the complexities of digital identity in Africa with a level of depth and collaboration that's rare to find.

One thing is clear: digital identity is at an inflection point. Some key takeaways:

- Identity & Payments Are Converging:
The lines between payments and identity are blurring as fintechs, telcos, and non-banks redefine trust.

- Innovation Outpaces Regulation:
Technology moves fast, but compliance lags behind—Integrated Identity Platforms (IIPs) could bridge security, compliance, and user experience.

- Organisational Identity & Chained Credentials Matter:
Businesses and institutions need verifiable identities too! The Global Legal Entity Identifier Foundation (GLEIF) vLEI standard enables organisations to prove their legitimacy and relationships through chained credentials.

At Vera, we hosted a session exploring two key debates shaping Africa's digital identity future:

📌 DIDComm vs. OID4VC

While both enable Verifiable Credential (VC) sharing, their approaches differ. OID4VC (built on OAuth) is easier to adopt, particularly for enterprises and governments, while DIDComm supports broader decentralised applications and peer-to-peer messaging, which offers Africa a more flexible and resilient path.

📌 Africa's Identity Standards: Follow Europe or Forge Its Own Path?

With infrastructure gaps and regulatory nuances, adopting eIDAS wholesale may not be the answer. Instead, Africa has an opportunity to create fit-for-purpose standards, just as South Africa developed POPIA instead of directly adopting GDPR.

This is only the beginning - DID:UNCONF AFRICA reaffirmed that Africa isn't just adopting digital identity solutions; it's shaping them.

A huge thank you to Gideon Lombard, Lohan Spies, and the DIDx team for an exceptional event. We look forward to what's next.



Event Highlights Photos and Testimonial Videos

You can see the Inaugural DID:UNCONF AFRICA Event Summary here: https://didunconf.africa/past-events

DID:UNCONF AFRICA 2026

DID:UNCONF AFRICA returns to STIAS, Stellenbosch, from 24–26 February 2026. Registration opens soon!

Visit www.didunconf.africa for updates or email info@didunconf.africa for more information about attending and sponsoring. Stay tuned for updates via email, LinkedIn, and our other channels—we'll be sharing news, programme highlights, and ways to get involved.

DID:UNCONF AFRICA is a Partnership between DIDx & IIW Inspired Regional Events

Open Space unConference Facilitation: Heidi Nobantu Saul
Notes Collection & Compilation: Heidi N. Saul