APAC Digital Identity unConference 2023 THAILAND

Book of Proceedings

Digital Identity.
one building block at a time

www.apacdigitalid.org

Thank You! Documentation Center & Book of Proceedings Sponsor: AyanWorks

Documentation Center
Sponsored by

Contents

About the APAC Digital Identity unConference

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

Open Space unConferences are particularly generative, with a facilitator we will co-create the agenda live each day of the event. There are no keynotes or panels, it's all about exploring the topic with professional peers from a range of identity areas.

Digital Identity is a keystone for a digital society and economy.

- Who are the people?
- What are the Organizations?
- Where are the things (products, commodities, shipping pallets) and where did they come from?

There are many reasons that secure identity systems are needed for connecting to others, tracking trade, supporting labor markets, crossing borders. Significant investments have been made into the development of interoperable standards, protocols, systems application layers, conceptual use cases, and more.

Who is this Event for?

This event is for individuals, practitioners, researchers, regulators, implementers, government leaders, technologists, digital and privacy rights activists. A neutral event where people from a range of different standards, efforts and businesses can come together, learn from each other, build connections and move the work forward

- Anyone who is implementing digital identity technologies, in government, enterprise and civil society.
- Startups working on emerging digital and decentralized identity technology
- Enterprises who are exploring digital and decentralized identity technology
- Ecosystems of interoperability are a key emerging topic and companies cultivating networks of interoperability
- Government leaders seeking to understand digital identity technology choices
- Those new to the concepts of Decentralized Identity and want to learn what it is all about

Event Background

The **APAC Digital Identity unConference** is inspired by the Internet Identity Workshop (IIW). The two facilitators and producers of IIW, Kaliya Young, Identity Woman and Heidi Nobantu Saul are collaborating with a local partner **Newlogic** to host and produce the event.

The time is right to host an event for the APAC region with the same Open Space unConference format that the Internet Identity Workshop uses. This event will bring together innovative startups and bold large companies who are building products and developing services using emerging digital identity technologies. One of the goals for the event is to foster a more connected ecosystem of companies working in the APAC region.

How an Open Space unConference Works

This is a participatory event and we will co-create the agenda together live each day of the event. There are no keynotes or panels, it's all about exploring the agenda topics with professional peers from a range of identity areas. All sessions are breakouts, and the topics are chosen and led by participants.

Through dozens of sessions, lunches & two evening meals **Provided by our Generous Sponsors** (all included in the ticket) you'll have plenty of chances to exchange ideas and make new professional connections. The Open Space unConference format is perfect for a rapidly moving field where the organizing team cannot predetermine what needs to be discussed.

We do know great people who will be there and it is the attendees and their passion for learning and contributing to the field of Digital and Decentralized Identity that all combine creating a successful event.

Read about how to prepare for an unConference here.
Read more about Open Space here.

Thank You to our Sponsors!

APAC Digital Identity unConference 2023 THAILAND

Supported by

THAILAND MICE | TCEB

THAILAND MICE TO MEET YOU Y2023

Special Thanks to Our Sponsors

NEWLOGIC

gluu

OPEN DEVELOPMENT INITIATIVE
AN EAST-WEST MANAGEMENT INSTITUTE PROJECT

AyanWorks

19 YENAKART
EATERY & GARDEN

WORKSHOP

CAFÉS RICHARD

Ronnefeldt

Vittel

This first APAC Digital Identity unConference would not be possible without the Sponsors who stepped up to make this initial gathering feasible. If you are interested in becoming a sponsor for future events, please contact

Daily Schedule

WEDNESDAY 1 MARCH
Welcome Reception for all Attendees
18:30 - 20:30 hrs.
Drinks and Canapes at **19 Yenakart - Eatery & Garden**

Sponsored by
Newlogic, 19 Yenakart and WORKSHOP

THURSDAY 2 MARCH
doors open at 8:30 hrs.
Light breakfast with coffee/Tea

Welcome & Introductions	9:30 - 10:15	Session 3	14:00 - 15:00
Opening Circle / Agenda Creation	10:15 - 11:00	Session 4	15:00 - 16:00
Session 1	11:00 - 12:00	Session 5	16:00 - 17:00
Session 2	12:00 - 13:00	Closing Circle	17:00 - 18:00
Lunch	13:00 - 14:00	Conference Drinks & Dinner	19:30 - 21:30

Conference Drinks & Dinner for all Attendees
Sponsored by
Newlogic, Gluu,
WORKSHOP and Pinnacle Gastro

FRIDAY 3 MARCH
doors open at 8:00 hrs.
Light breakfast with coffee/Tea

Opening Circle / Agenda Creation	9:00 -9:30	Lunch	12:30 - 13:30
Session 6	9:30 - 10:30	Session 9	13:30 - 14:30
Session 7	10:30 -11:30	Session 10	14:30 - 15:30
Session 8	11:30 -12:30	Closing Circle	15:30 - 16:30

No Host Post Event Dinner
Location to be recommended by Newlogic Team!

APAC Digital Identity unConference 2023 THAILAND

Fostering innovation & collaboration between emerging digital identity companies and projects across the APAC region!

Agenda Creation = Sessions Called and Hosted by Attendees

25 distinct sessions were called and held over 2 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work for all 25 of these sessions.

Thursday March 3, 2023 ~ Day 1

Session 1
1A/ Asian n/w for DI standards / Ujjwal Deep Dahal
1D/ Sri Lanka's Digital ID - MOSIP Implementation / Dasun Hegoda
1E/ Cross - Border Travel Without Passports - Navigating Digital ID Recognition Across Borders / Eric W & TY

Session 2
2A/ What Constitutes Indigenous ID in SSI Approaches? / Pru
2D/ PART 1: What is the Decentralized Identity Foundation {DIF}
PART 2: Explore/Map the .orgs & Working Groups in the Identity Ecosystem Globally & in APAC / Kaliya and Catherine

Session 3
3A/ Open Discussion on Blockers for Mass Adoption and How to get Around Them
3C/ Pictures as Identifiers

3D/ Building Identity Journeys with Low Code

Session 4
4B/ Inclusive ID - Please Define! / Puneet, Jeremi and Pru
4D/ How a Cloud Wallet Can Bridge SSI to Normal People / Mike S Gluu
4E/ Data - Centric Digital Rights (DCDR) Framework / Jean

Session 5
5A/ Open Discussion - Singpass - Singapore's National Digital ID / Yee Noi
5C/ 2D "Not QR" Codes + Civil Registration + Vital Statistics / Eric

Friday March 3, 2022 ~ Day 2

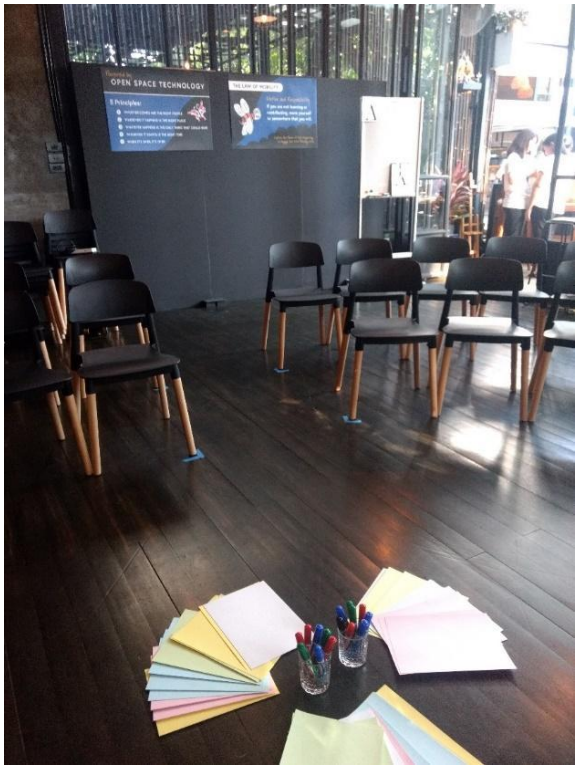
Session 6
6A/ (ToIP) Digital Trust Ecosystems - Components, Mental Model - Looking for Feedback / Eric D

Session 7
7A/ Identity & Domain Names / Gihan
7B/ As a Newbie (weather technical or non technical) What are the ways I can engage to be able to implement SSI?
7D/ Whiteboard Session: Elements That Make APAC Trust Framework / TY

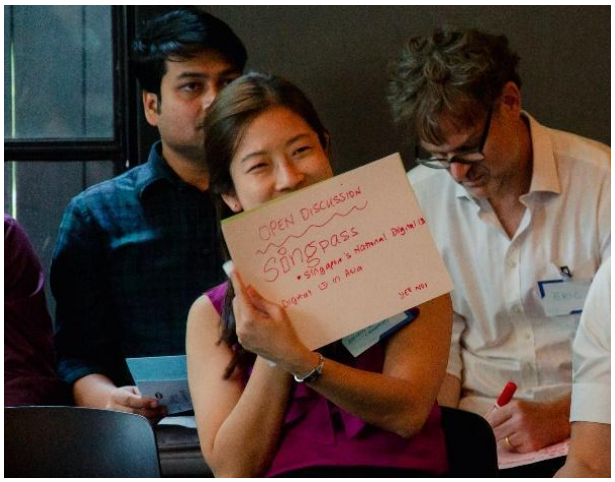
Session 8
8A/ Building Open Source Communities + New Ideas / Mike and Dhaval
8B/ Verifiable Identity: Social Media - "The Bali Process" Context: Human Trafficking Transnational Crime / Eric D
8C/ Our Journey to SSI in Thailand (use cases & poc Call for Collaboration) / Finema - Catherine

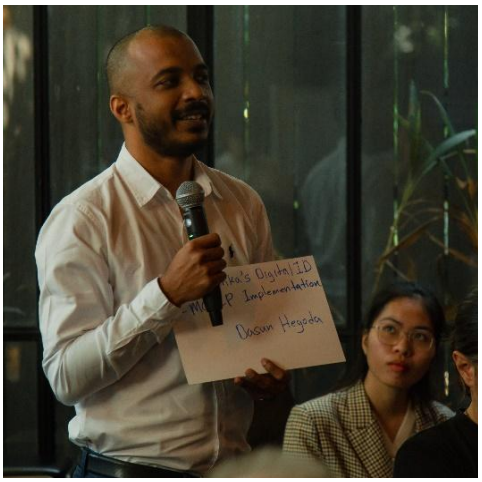
Session 9
9A/ Blue Economy and Regional paperless trade / Eric W
9D/ Share the Journey of IAM Delivery Work - do's don'ts Lessons Best Practices/ Dave Y
9E/ Analyzing Structured Datas LIfe Cycle / Jean and John

Session 10
10A/ NFTs as an Identifier - Pro's Con's Is it worth it? NFT adoption and applications / Mike - Victor
10D/ Verifiable Credentials - Exchange Protocol and Wallet Interaction / Ashish T


OPEN SPACE TECHNOLOGY


What constitutes


OPEN DISCUSSION
SINGPASS


Dasun Hegoda

Session Notes Day 1 / Thursday Day 1 / Sessions 1 - 5

SESSION #1

Standards for Distributed ID for Asia

Session Convener: Ujjwal Deep Dahal
Session Notes Taker: Victor Ocampo
(optional) List of Session Attendees: Ujjwal, Puneet (mosip.io), Davin, Kirankalyan & Ajay

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Ujjwal is the CEO of Druk holdings, Bhutan's investment arm, like Singapore's Temasek
First govt to implement an SSI-like DID in the world delivered via mobile
Govt still issues SID but control is with individuals
Tx creates a DID record in the blockchain of their foundational ID
Authentication is decentralized

Puneet - introduced nonprofit MOSIP
Modular Open Source Identity Platform (MOSIP) - digital, foundational identity system in a cost effective way.
From the International Institute of Information Technology
Uses Biometric Standard called e-signet

Discussion ~ Requirement to have SSI/DID standards across APAC
Maybe modelled around the Asian Football Federation

Issues:
Is there such a thing as a true SSI?
The only true SSI is one thats is issued by you as an individual

How do you serve the underserved?
Mosip- Qr code - physical.code
Bhutan foundational did given in mobile

How important is policy in implementing an SSI
It is inescapable.
Still need a certification authority ~ Data is always with the issuer

Others
Blockchain based ssi is not practical
No Biometric Standard for ssi
No protocol to accept virtual certificates

Next step - convene an Asia-wide conference on DID standards

Sri Lanka Digital ID - MOSIP(Modular Open Source Identity Platform) Implementation

Session Convener: Dasun Hegoda
Session Notes Taker: Ashish Tripathi
(optional) List of Session Attendees: Geun-Hyung Kim

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Open Source platform for Identity management in Sri Lanka with MOSIP. They are ICTA.

Classification of govt ID

1. Foundational ID - framework provided by the government.
2. Functional - entities use the above framework and build Identity solutions. e.g. Driving licence.

Example, citizenship is created by the Government and a Driving licence is issued (by different authority using functional ID) using this ID.

Eliminates redundant data from the ecosystem. That is, they collect data once and share it with everyone (but it is authorised access only).

Architecture

Lanka government network -> Lanka government cloud -> Digital identity -> National data exchange -> departmental consumption.

Hybrid model for deployment for different entities, based on the requirements. So for some they use government cloud and some deploy / replicate it for convenience.

Services are REST APIs.

Trying to add consent based data sharing.

All data consumption is through API requests, the service application doesn't store locally.
For data standardisation, it relies on ISOs.

They did a POC(Proof of Concept) with MOSIP, for basic registration and authentication.

Additional notes: Carmen Lam

3 levels of data classification:

- public data
- protected data (accessibility to this kind of data based on the role or function of the requester)
- private data

Government agencies access citizen data in the system through trusted service providers (TSP) that are licensed by ICTA.

Based on MOSIP:

- no vendor lock-in
- lower cost

To be inclusive:

- the digital ID system also provides users with physical ID cards.
- the application is available in three languages, English / Tamil / Sinalese

Open Discussion: Navigating, Recognition Across Borders / Cross Border Travel Without Passports - Navigating Digital ID Recognition Across Borders

Session Convener: Tze Yuan & Eric Drury
Session Notes Taker: Yee Noi & Merul
(optional) List of Session Attendees: Jacques, Dhi, Deng, Eric Welton, Sang, Keng, Chol, Pyro, Dru, Nihi, Sophia. Jean

Please list the key points of your conversation and/or what you would like to share with your colleagues.

How to trust CA, VC?
CA: Certificate Authority
VC: Verifiable Credentials.

Points of Discussion:
Trade Zone identity: Case of Bhutan and India.

- How to manage of the 2 way border crossing is done?
- Managing the high capacity
- Maintaining privacy, security and rights of the individual → Me as the owner of data.
- Anyone needs/service to ask me for the information necessary to fulfil the service.

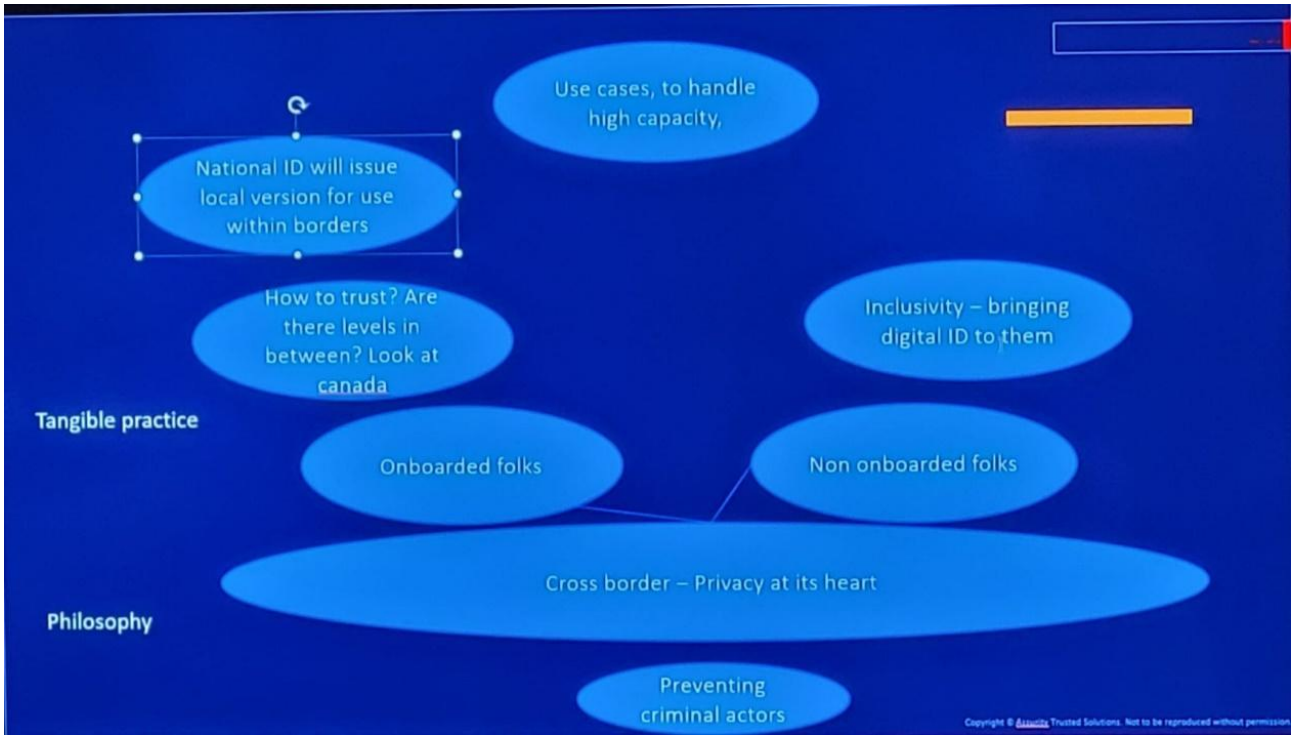
How to trust cross border - trust the people who build the environment?

- Cross border engagement with divergent trust and different digital technology levels.
- What is minimally viable for it to happen?

Include people in digital identity rather than compromise security.

- provide tokens etc
- (Important) Educating people understanding reason why the identity if important.

Providing credentials to do something, need not be identity.



Summary:

- Singapore has an app called singpass, more than a credential and goes even more than just the bare fundamentals
  - shows id cards and other claims
  - share using bare code and Face Recognition
  - The Authentication and Signing Certificate are the proof in the digital world
  - Banks and institutions have tried to use id but with a very patchy manner
  - gaps are created because a foreign verifier will have to trust the CAs and VCs and the Data Networks and the underlying protocol
- IOM (International Organization for Migrations):
  - sovereign nations are responsible for their identities
  - governmets need to have trade frameworks which do not rely on the heavy infrastructure of passport
  - IOM is interested in understanding the solutions
  - Bhutan-India have a treaty for citizens to move accross borders with any of the country's documents
    - Working on an edge wallet which allows you to store digital versions of the country's documents
    - The app has a Bhutanese foundation ID and also allows to store foreign claims as well.
    - 12-13k people pass an hour, presenting a document is too much of a hassle
    - The claim is issued as a VC by three government entities
    - everything is SSI based except the foundational ID (government ID) is issued by the government
    - wallet is free and given to everyone
    - 5 variants: digital wallet runs on the phone, fingerprint usb stick, printed QR code, custodial wallet, cloud wallet

- To save the hasle of accidentally destroying the wallet, you consent for a backup, the backup is stored encrypted and sharded into 7 chunks on the database
- Countries without DID at the moment (think Congo and Zambia)
- From the PoV of an already working system, the mobile onboarding needs two identities, a picture identity (government issued)
- Map humans: levels of trust with identities, verify with the local authorities
- Risk based excercise, stricter on higher risk scenarioes, more laxed on things like tourists
- currently takes 1:30 minutes automatically and issue a digital claim
- the whole model was created to be exportable and can be replicated globally, most of the core tech is service like
- working on a national id which will become an act later through the parliament
- the entitiy will be a Non-Government entity and the board will be air-gapped from the government so as to prevent government from steering the direction of the project too much in any specific direction
- anyone can only ask for the data that they can prove that they actually need to serve you (it is built into the app)
- you can't keep the data forever and can only keep it to a certain time and the user can request to remove data
- Minimum Viable Governance for the context, governance can have a bazillion frameworks in place but what is the minimalistic approach to a certain scenario
- How can this system help with bad things like Human Trafficking
- Educate the public how your identity benefits you so as to not share
- localised guiding and onboarding process in local languages to help farmers onboard

SESSION #2

What Constitutes Indigenous ID in SSI Approaches?

Session Convener: Pru
Session Notes Taker: Merul

Please list the key points of your conversation and/or what you would like to share with your colleagues.

- Indigenous people have rights to self determination and are considered sovereign
- the way they identify and attach themselves is closely intertwined to the land they originate from
- Existing works like technological and government frameworks which pre-exist
- How do you adapt SSI and integrate indigenous people onto that
- How do you integrate aspects of indigenous culture into the whole angle of SSI
- Indigenous people in South East Asia constitute ~4.9 Million People (outdated census)
- Self identifying with that of an indigenous person is very deadly
- Countries get around by saying that they have never been colonised, UN convention frames it around external colonisers but truthfully asian countries have had internal colonists however technically asian countries are complying
- Malaysian and Vietnamese identities are scary as they might disenfranchise the indigenous people even more
- lack of political will
- Organisational clamp on indigenous people, the moment you take an official document your rights will be taken away, as an indigenous person you get no access to education and healthcare however the document waives away your indigenous rights
- Soulbound tokens, tie it like an NFT and if you lose it your community can help recover it for you
- the technology which underlies the whole ecosystem is open source
- Proof of Humanity (SC where you as a human submit biometrics, the name and the bio, another member accepts and validates)
- Separate the Ethnicity of the individual from the foundational identity and that could be further declared and imposed with another proof
- who watches the watchman (nice research paper to study)
- NCIP (National Commission of Indigenous People) in the philippines is the only asian entity to exist in this context
- cross ethnicity marriage

Decentralized Identity Foundation (DIF) & the Broader Ecosystem of .orgs

Session Convener: Kaliya Young, Catherine Nabbala
Session Notes Taker: Ashish Tripathi & Kaliya Young
(optional) List of Session Attendees: Geun-Hyung Kim

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Decentralized Identity Foundation (DIF)
Is a not for profit, member driven open standards development and technical community, building foundational elements of the decentralized identity ecosystem.
More about DIF: https://identity.foundation/

Decentralized Identity solves challenges in many fields including:

- Open Banking
- Open Government
- Trade
- Immigration

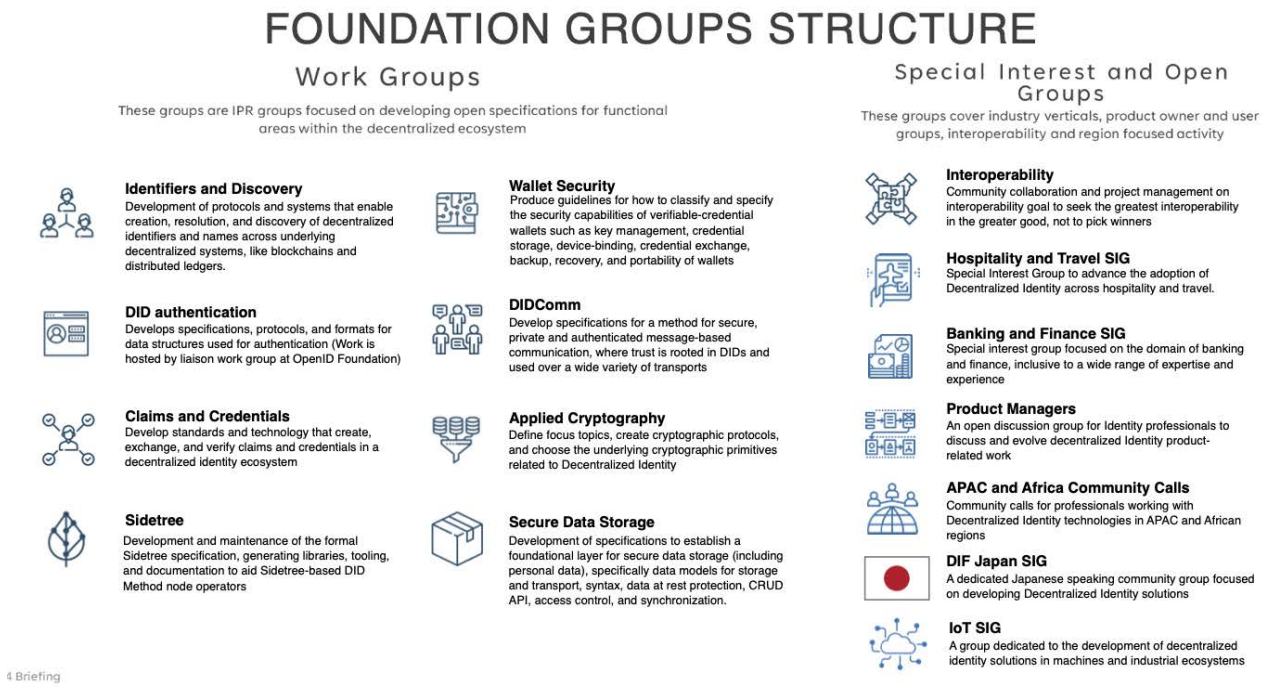
Kaliya has a weekly Newsletter about the industry.
https://newsletter.identosphere.net/
You can also read about her work at
https://www.identitywoman.net/

DIF has been running initiatives in the Identity space for a long time and have been associated with open source work.

Decentralized Identity :

1. One of the key challenges is that all legacy systems involve userID and password to access, and are being used by enterprises and its users.
2. For citizenship credentials it becomes difficult to associate it with legacy systems and the way they can be issued and maintained.
3. Identities should be able to align with all sorts of requirements and use cases, not just accessibility and enterprise data.

They are non profit and member driven open standards.



Applied Cryptography is focusing on signatures, new reference implementations and standards like BBS Signature.

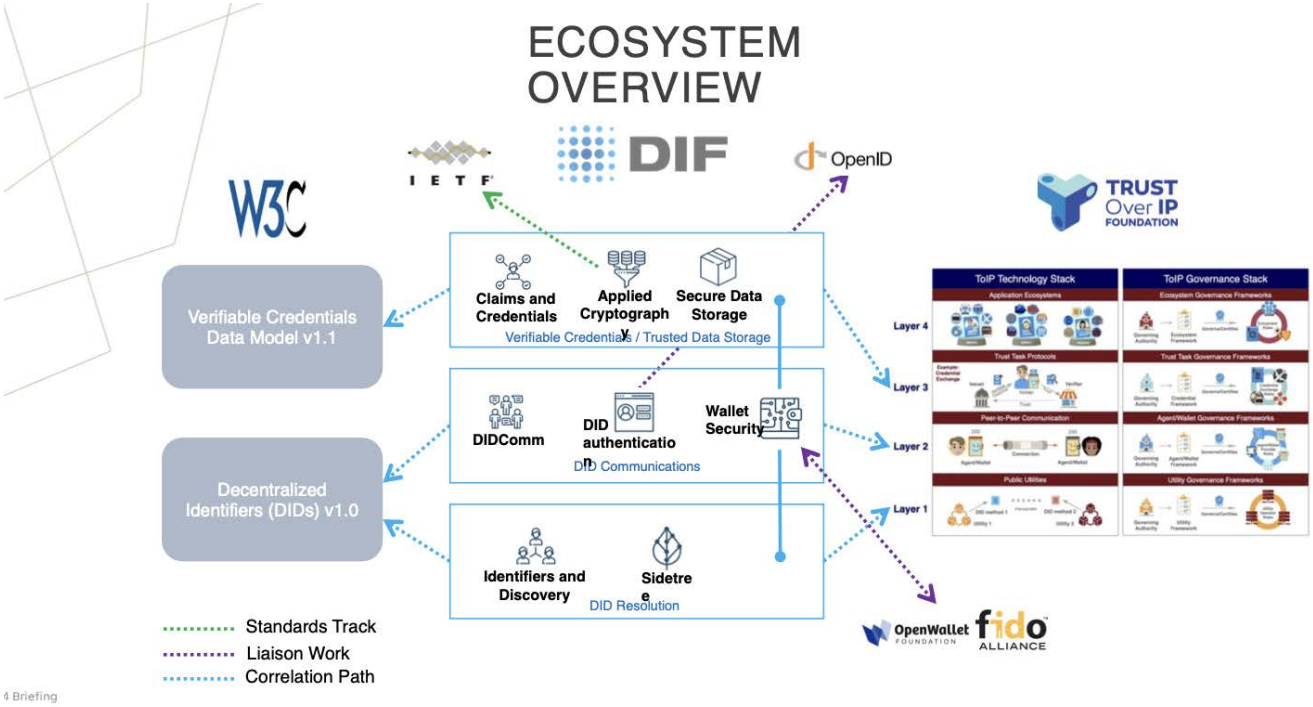
One can join different working groups and special interest groups. However, IPR is needed for working groups. Calls are arranged for different time zones.

Organisations can join as Members or Contributors. See the differences here

Individuals with no direct employment can join using the Feedback Agreement. Learn more here

Foundations / Agencies. Please get in touch via membership@identity.foundation

Please check the website to know more about membership. Website - https://identity.foundation/



Decentralized Identifier :

1. Anyone can get a DID.
2. This can be shared with anyone and be used for different purposes.
3. DID have `method` and `cryptographic keys`.

   For example, a college degree use case.

   1. The student has a DID and this DID is registered in the Verifiable Data / DID registry.
   2. The college is registered in Trusted Registries.
   3. The college issues a Degree (Verifiable Credential).
   4. This VC degree has a proof of issuer.
   5. The student presents that VC in the form of Verifiable Presentation to the employer. The VP has the signature of the student on top of the VC.

Some docs to understand DID and exchanges :

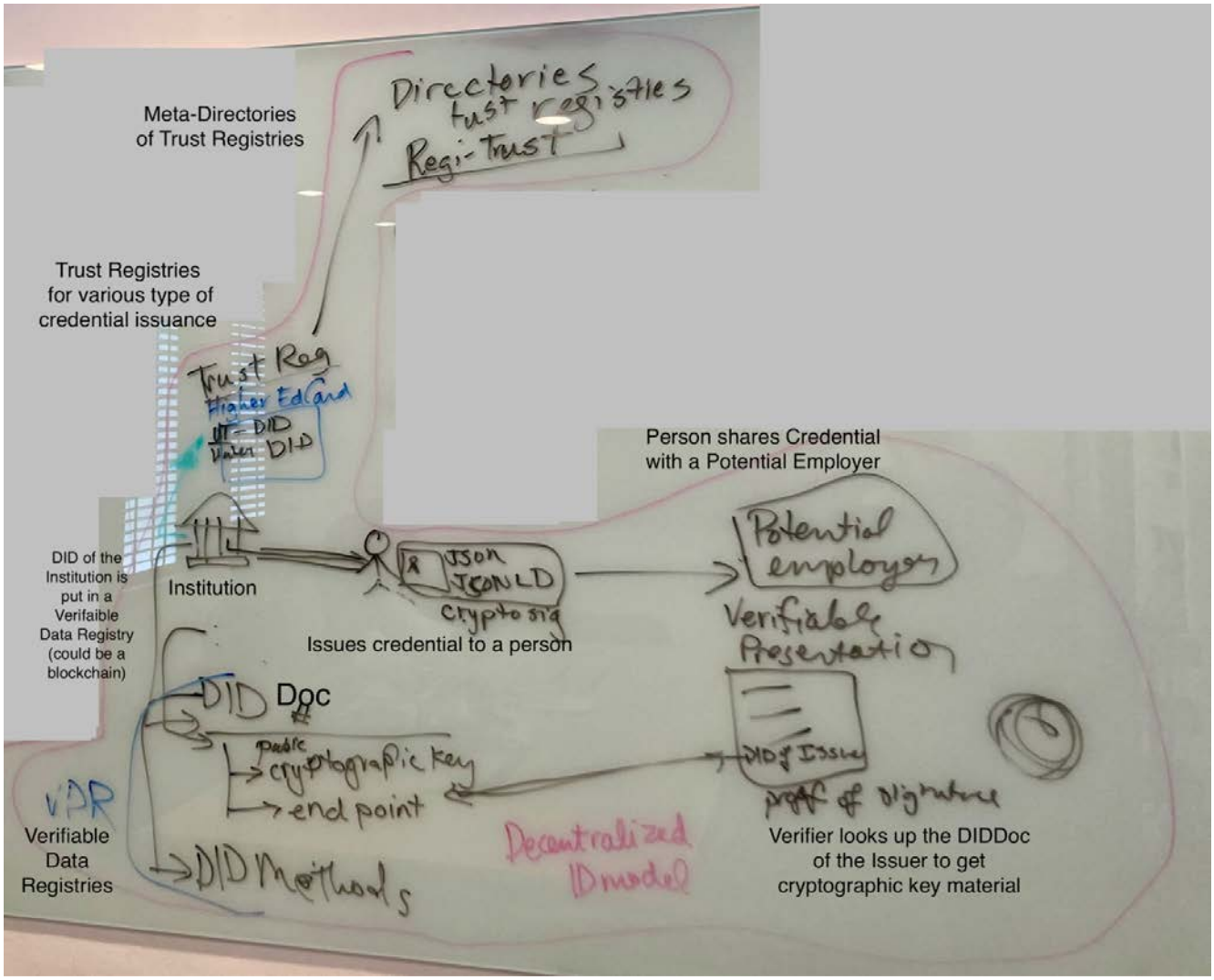
1. https://github.com/energywebfoundation/ssi/tree/develop/apps/vc-api/docs
2. DID specification - https://www.w3.org/TR/did-core/
3. Verifiable Credentials - https://www.w3.org/TR/vc-data-model/

Could we have an ASEAN of eIDAS2?
Example in the real world at scale TruAge put in place across 150,000 convenience stores in the US via their trade association NACS.

We white boarded

Old centralised and federated model - with phone home architecture like OpenID or SAML.

Decentralized ID Model White Board



Organisations within the Linux Foundation

- Decentralised Identity Foundation is under the JDF
- Trust over IP Foundation
- Open Wallet Foundation
- Content Authenticity Initiative

We white boarded several of the different organisations working on digital identity

- OpenID Foundation
- Kantara Initiative
- FIDO Alliance
- ID2020

- ADIA
- MOSIP
- OpenCRVS

SDOs

- IETF
- ISO
- IEEE
- ICANN - IANA
- ITU-T
- IATA
- Eth Foundation

Join the APAC DIF Call to connect in an ongoing way with the community - sign up here.

SESSION #3

Open Discussion on Blockers for Mass Adoption and How to get Around Them

Session Convener: Merul
Session Notes Taker: Unknown (1st set) Kaliya Young (2nd set)

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Tangle Labs used to provide consumer facing solutions re: DID, SSI, Verifiable Credentials
Ticketing Scene: Ticket Master is terrible but there's no alternative
Consumers follow the path of least resistance and they don't want to deal with additional steps
In crypto, you become your own bank which is not appropriate for a lot of consumers
Controlling your own wallet has its own responsibilities which they wouldn't be able to perform or even is willing to perform.

Is SSI just a tech utopia?
Authoritative Issuers can revoke a card or reissue a card.
If you have 10 credentials in your wallet, they won't be able.
They can't restore your wallet.

Bhutan - Foundational ID. Opt you in to backup and restoring your wallet. Restore the version that the government have. Treat the wallet as a blackbox item; zip it then shard it out. Edge wallet on your phone.

Encrypted Data Wallets - wallet for things; in the cloud.
Spend a lot of time on marketing and user education. QR code for bank transactions.
National Day - app with money incentives. Pandemic response - is distributed through the app.
SSI just last year.

What is a level that is good enough that will drive adoption?
In government → National ID, Driver's Licence
In the private → Banking, Open a bank account in 5 seconds

Identifying a Minimum Good Adoption Level as a driver for decision on Go Live
Educate people on the benefits.
L1: Sign in / authentication
L2: Paperwork / KYC
L3: Simplifying the process / integration across systems

Can a startup really do anything to drive SSI? You can't.
It's really about ecosystem. Go find X entities that need each other and figure out how to provide benefits for the end-user which would be enough to jump start an ecosystem.

Don’t sell SSI. Sell solutions, sell benefits and value and build it in SSI manner.
Don’t use SSI as a word because that might scare off people who might be scared about losing power.

Separate marketing-speak from solution-speak. We removed all references to SSI / Decentralized.
Eventually, you want consumers to be familiar with the underlying technology. People are least bothered by privacy. But there is a good chunk of population also cares about privacy.
UX issues

- Use cases
- User Experience

Not everyone would have the potential to understand the solution.

Is SSI practical idea or
We have to empathise with our core users.
Not the technology enthusiast.

What would be the ideal middle ground to begin towards the SSI model.

How are the products used?
Custodian solutions - stored on cloud.
Wanted privacy angle.
Wanted someone else's responsibility.
People don’t want to lose.

We started out doing products for people.
But then how many steps to get credential?

- get a wallet - do the custodial things

With Government issued credentials how do you get a new one if you loose your phone?

Example shared from Bhutan
Issue credential.
On-boarding for it.

Opt you into restoration and back-up - opt-out (so unless you opt out it is backed up).

Then if you come back you can get a restored version.
As long as can’t get into wallet to do restoration.
We can’t remind you all the things you have.
Most people don’t want to do backup/restore.

How does the backup work.
Take wallet - take it table - object. Shink - encode - chard - bread crumbs and 7 databases.

Trigger in wallet - trigger - backup.
Wallets have to back up.

Actively discuss.
What is the balance - to push out consumer facing applications.
Provide them with utilities and

Make viable

Jaques (from Bhutan) talked about political will and building it.
We spent a lot of time on marketing and education.
Did a lot of time to get people to understand and feel good about it.
QR code digital money transfer.

With the National Day.
You can buy a ticket for that event - either with the wallet or a paper one.

People were Incentivized for getting the app because they got things for free.

Download application and get loan - didn't have to pay it back. (but if you did you could get another lone)
Digital is good - see real benefits.
Digital Keedo
This familiarity with digital and money payments made it simpler for us to introduce SSI.

Provide and identity - do every day subscribe to national day.
By accident or pre-planned.

It is a journey - his majesty - said that they have to adopt it. Working with Ministries have to really move ahead.
Private sector sees the benefits.

- real thing.

Comment from audience - I should introduce you to the HongKong Government

We didn't pick a date to go live.
What is a level is good enough to go live that adoption will come.

These digital services in government must be integrated. Need every month -
Banking application adoption.
Not chasing a date - level of issuers and verifiers on the platform that guarantee adoption.

How do you think the private sector individuals and organizations. Bringing out consumer solutions.

How do you think without that huge force could reasonably drive adoption.
Benefit to consumers.
Don't want to download an app - know they will use every day 50 times in the next year.
Not have to fill out a paper form.

“open bank account” in 5 seconds.
2.5 months now to open a bank account now on paper.

Bank can’t take any more information they they are permitted by law.
Gives trust to people. See in every day life.
MBot - must put in pin-code and password - doing passwordless login with SSI.

3 layers of integration.
Layer 1 - using national digital ID to sign things.
Layer 2 - top filling in paper forms.
Layer 3 - changing work processes –

Question: Can you do SSI with a small company driving consumer adoption?
the answer is you “can’t”

It is a team / ecosystem sport.

SSI is a means to an end - not the end itself.

Ticket Master - sistic (Singapore - ticket master)

Benefit/pain. (like going to a BTS concert)

Provide enough of a value - provide value to consumers.
Enough to deal with hassle.
Because I want to get to that point.

We agree that it is NOT easy.
problem - people is data is power and knowledge. Every department still have information.

They have invested in “a” system.

Separate Marketing speak from solution speak.
Trying to promote it within the company - disappeared all references to SSI and Decentralized.

If able to explain product to customer without using any of those terms then you are successful.
You want consumers to use the wallet - enrol with the wallet.
How simplified is the process to keep then engaged.

KYC to be done - scan Driver Licence.
Probably want to keep that and specific services.

Do we need to market to consumers how they - Privacy being preserved.
India context - not concerned about privacy.

Germans care about privacy

Keep it simple.

If your product the only value is SSI -

Eric - have you talked about UX.
Not yet.

We had a lot of discussion in Trust over IP foundation
Trends in
Tech stack - they're sort of ready.
Before you get there what is a really well defined use-case - well defined problem - better cheaper?
Once agree to go forward - what is the UX - has been really pretty poor.
Wait I have to sign in differently - to many steps.

Book ends - have been blockers

- Use-Case
- User-Experience

Implementation
Proving a lot.

Before we (TangleLabs) got into issuing claims for educational institutions.
Trying to replace TicketMaster - had to download wallet - set it up - mnemonic etc.

Maybe you go to a concert once a year - don't want an app just for that.

Digital Identity or SSI or way do it today.

How do we solve fundamental problem of humans -
Don't have "an Identity" don't have resources.
Really working to solve a fundamental problem. 16.9
Distributing resources to the poor.

Working at social point - going for mass implementation now.
Other point is sometimes certain things - need to be told this is the best way to go.

SSI is probable something can push as betterment - identity problem.

Good portion do care about privacy.

Pictures as Identifiers

Session Convener: Gihan
Session Notes Taker: Eric Drury

Please list the key points of your conversation and/or what you would like to share with your colleagues.

This session pondered whether images - linked to specific people, or organisations - could be used as ID?

For example, many organisations have logos, and when online, perhaps these logos are clickable which points to a URL. Or people may have profile pictures, images, avatars, … that could be unique to them.

The question is: is there a way, a use, a need to allow us to create images that can then be verified as linked to individuals, or organisations? Can we do something similar to the way Google image search works – where we upload the image and it shows us the details of the individual or organisation which "owns" that image?

Can we do that in a more formal way? In some way that is not completely deterministic?

Can the process be automated?

Can we use this to determine whether a company is entitled to use that logo on their website?

Question: can this approach be used with IP?

Question: In indigenous communities, sometimes tourist organisations use indigenous artwork, or indigenous 'culture' – but do not attribute that artwork to the community? Can this approach help address this problem?
How can you track if people are using your image that you own?

Would this be similar to IP registration? Or an NFT?

Is it feasible to try to track everyone that's using that image, and then figure out whether they have permission? What about the 'white list' approach?

Why not use something not the picture, why not use the digital identifier.

Written in particular font, or pictogram?

This is an interesting problem to solve, especially with the arrival of the Metaverse, where we only see images and need to be able to know who or what that image is attached to.

Identity Journeys with Low Code / Gluu

Session Convener: Mike Schwartz, CEO Gluu
Session Notes Taker: Ashish Tripathi

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Modern authentication has evolved. In the old days, we would present one web page to a person (normally a username password form), process it, and either allow or deny access to the website. Today, modern identity services use a series of web pages to authenticate a person using a web browser. Frequently, the web pages displayed vary based on the security assessment. For example, if the authentication seems unusual--perhaps the person is using a non-recognized browser, or is logging in from a new geographic location--websites might want to use additional steps to make sure it's really the person.

But authentication is just one "identity journey". Social login, registration, "forgot password", two-factor credential enrollment, and consent are other examples. At a high level, we could categorize the three most typical identity journeys as:

1. Registration
2. Sign-In (authentication)
3. Forget password (credential enrollment)

Wholistically, this process for building identity journeys is also referred to in the security space as "identity orchestration".

As modern authentication is increasing based on open standards, especially OpenID Connect, the question is how can we enable websites to build these identity journeys as part of the OpenID Connect flow?

In the past, Gluu exposed a mechanism called "interception scripts", which were written in Java or Python syntax. These scripts were extremely powerful, enabling websites to build any type of authentication flow. However, writing an interception scripts required at least an intermediate level of programming skills. To implement more complicated flows, it was good if you were an experienced Java developer.

One particular challenge, regarding the maintenance of these scripts is knowledge transfer. The original author of the scripts has deep knowledge of how they work. But how does the original author transfer the script to the next team? As the scripts are asynchronous, there is no sequential way to read them. Basically, the new teams needs to expend a material effort to study and understand the code.

In the last few years, "low code" has emerged as a strategy to enable developers to use graphical tools to white board programs. Some platforms even make the promise of "no code" by providing pre-built components that perform all the tasks you might want to assemble to make a working

solution. But “no-code” solutions suffer from one disadvantage--if the platform designs haven’t provided the functionality, there is no way to accomplish the task. Because the requirements for building identity journeys are so diverse, a low code approach is better.

The Janssen Project, a Linux Foundation chartered group, was formed with the purpose to build a world class OpenID Connect provider. In 2020, Gluu contributed the open source code that it had developer since 2009 to provide an advanced starting point--the Gluu Server was the most certified OpenID Provider and was used in production by hundreds of companies, including a significant number of governments, financial institutions, large enterprises, and global security companies. Building on this, the project has continued to innovate rapidly, not just in functionality, but in tools to enable easy administration, cloud native deployment, and to increase the transparency and quality of the CI/CD process. The Github URL for the janssen project is https://jans.io

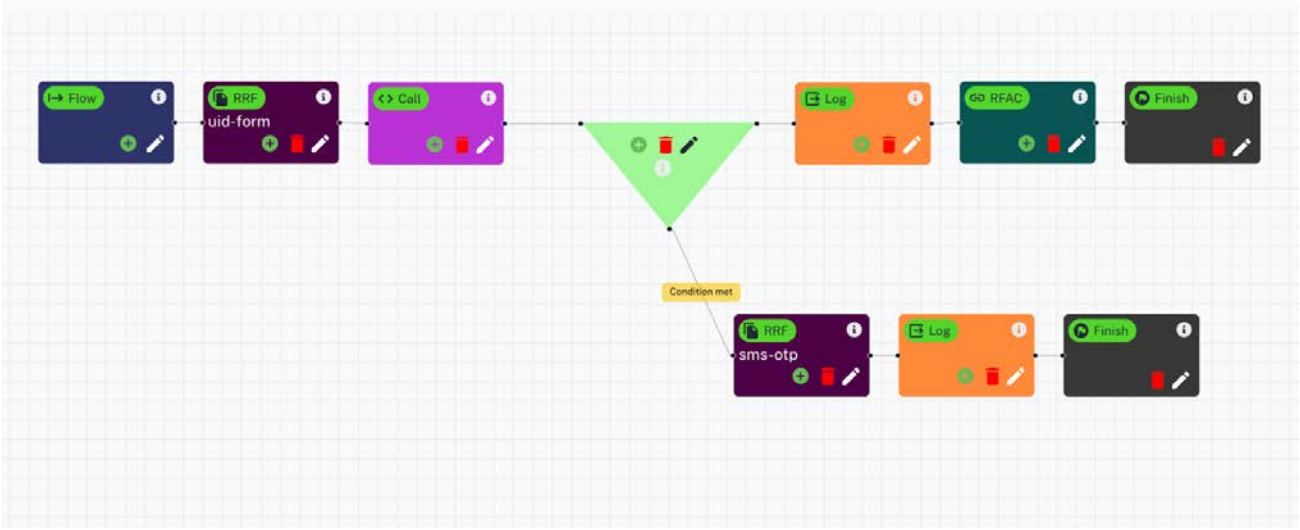
In 2021, the Janssen Project senior developers decided to build a low-code solution for identity journeys, after the success of similar platforms by large commercial, proprietary OpenID Connect vendors like ForgeRock and Ping Identity. There was no open source low code way to build these identity journeys, and the Janssen Team projected that enabling developers to use this approach would attract a large community, especially vis-a-vis Red Hat Keycloak, another popular (but difficult to customize) open source identity platform.

After surveying a number of possible solutions to build a low code identity orchestration solution, Jose Gonzalez, one of the lead developers at the Janssen Project, proposed an interesting idea: why not design a domain specific language, or DSL, that specifically addressed the requirements for building web flows for identity orchestration. This approach was ultimately selected, and Agama was born. (Mike Schwartz picked the name Agama based on a visit to the San Antonia zoo reptile collection, where he saw some cute shield tailed Agamas). You can find an introduction to the Agama DSL in the Janssen documentation:
https://docs.jans.io/head/admin/developer/agama/

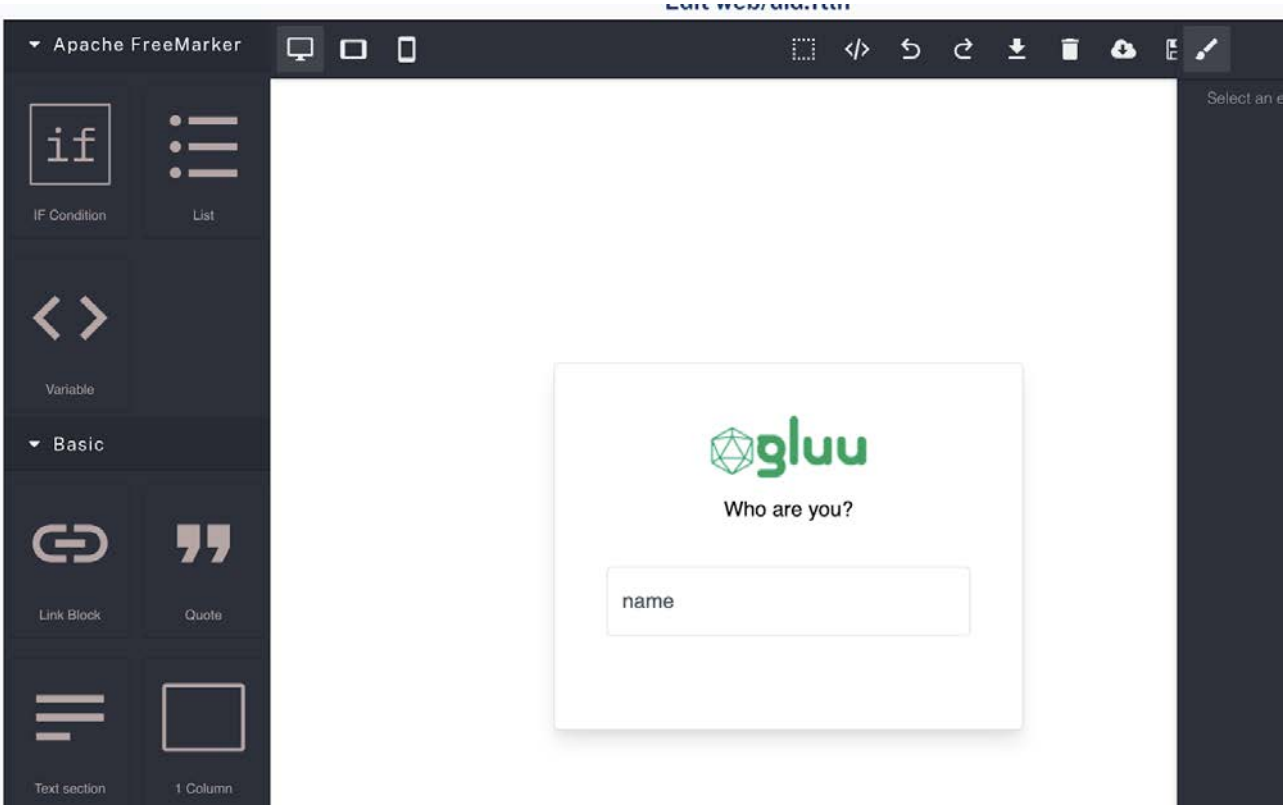
However, writing the Agama language was only the start. What was really needed to complete the vision was a developer tool that authored Agama projects through the use of low-code (drag and drop). This tool was launched by Gluu in February of 2022 on a website called “Agama Lab”, which can be found at https://cloud.gluu.org/agama-lab

While Gluu hosts the Agama Lab developer tool, it does not store any project assets--developer specify a Github repository where they want to save the files. Agama Lab creates a branch in the repository to save any changes. Note: Agama Lab does perform a Pull Request (or “PR”), merging the authored code to the “main” branch of the repository. Gluu did not want to interfere with the developer’s process to peer review code before acceptance.

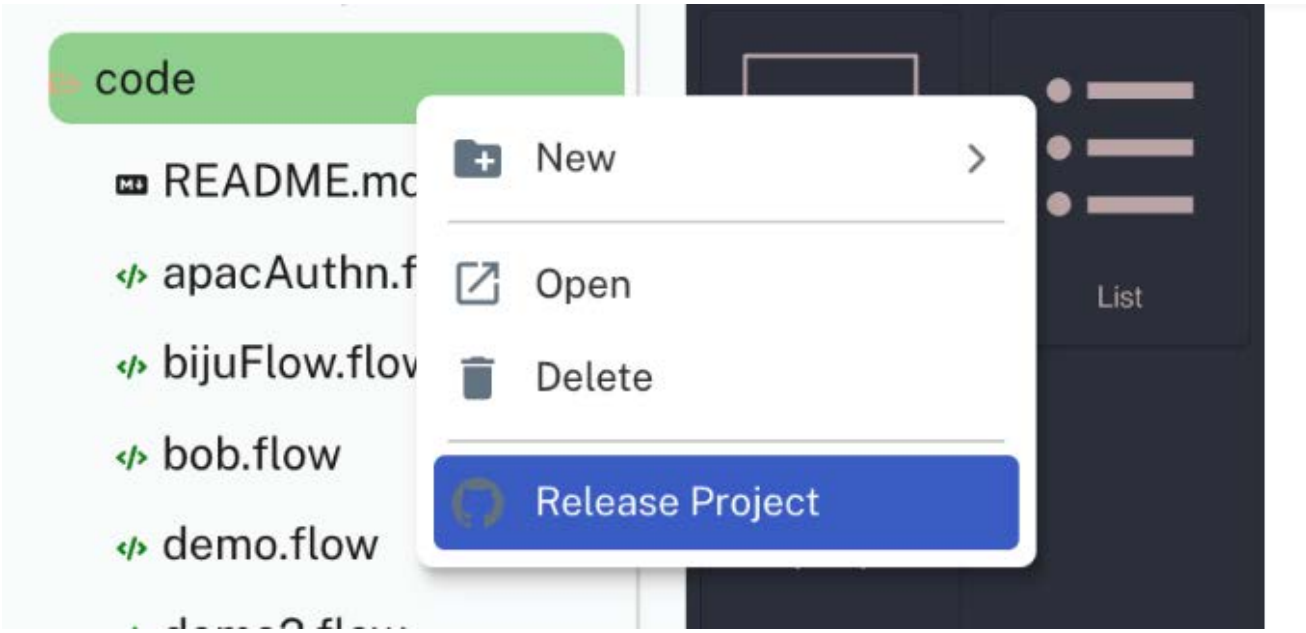
The Agama Lab authoring tool has a tool to enable developers (or architects) to whiteboard (or “orchestrate) the business logic of the identity flow--what series of web pages to display, under what conditions. And there is also a tool to design web forms. During the session, Mike authored a simple flow that stepped up authentication if fraud was detected. It looked like this:



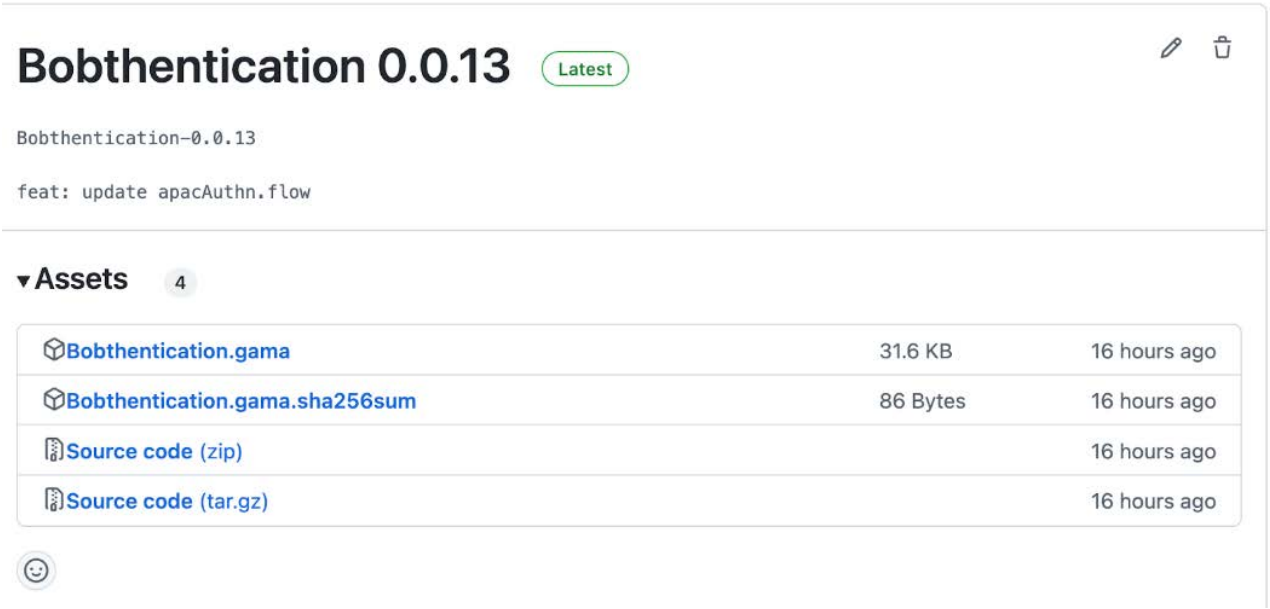
He also built a simple form in the form builder:



Once the project is completed, the Agama developer can “release the project”. In this process, Agama Lab collects all the assets for the project--the flows, forms, code, and assets (e.g. images, css, javascript)--and creates an Agama Archive, which is a zip file.



This release is published as a Github release in the developers repository, with a SHA256 checksum, like this:



Once the project is released, it can be uploaded to any Janssen Auth Server (or Gluu Flex Server), which auto-deploys the assets.

For a client to invoke an agama script using OpenID Connect, it must use `acr_values=agama` and then add a special parameter, `agama_flow=(name of the flow)`.

SESSION #4

Inclusive ID - Please Define!

Session Convener: Puneet, Jeremi and Pru
Session Notes Taker:

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Does inclusivity also mean giving people smart phones?

- Smart phones, feature phones, people that do not have phones
- OTP - Feature Phones
- USSP - Dial #123* to avail of services
- Kiosk - only needs ID number

No connectivity

- Offline Authentication
- QR code on the card, and you can verify biometric information from the smart phone that's scanning

COVID Credentials Initiative

JWT-encoded QR Code has a problem is that it's not obviously a copy. There are issues around identity theft.

Trilemma of Inclusivity

- Accessibility
- Security
- Privacy

There will be use cases wherein there wouldn't be internet access e.g. refugees.

Discussion re: refugees
United Nations had a paper system to establish identity to track you and then eventually absorb you into the hosting country. Nowadays, governments doesn't want you to be nationals. Now, they're giving you documentation to be able to track you to actually deny you services which puts you in a cage.

Aadhaar as a system
Significant issues of people being denied access to Aadhaar in Assam (region near Bangladesh).

How can you build safeguards against abuse of power in our identity systems?

Technology being used to trap/track people. How easy it is in decentralized systems to be able to track people?

Old model:

- Register with the system, issue an ID
- The system sees which systems you've interacted with by virtue of your ID

Decentralized model:

- Verifiers is only able to see your current identity
- There is still a possibility of verifier collusion

Bhutan: Education effort is still massive. 220 stakeholders, meeting every month. And yet there will be people that still want all the data. They equate data with power. But we have to educate them that you'll have enough data to be able to do your function.

Biometric companies seems to equate biometric = digital identity. Why do organizations have identity? How are people remembered by the institutions that they've interacted with?

Madison Square Garden facial recognition issue:
https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html

The Dark Side of SSI - the right to lie. Losing the ability to be ambiguous.

Inclusivity should also regard excluding some aspects and not strive to codify everything into digital.

Are we going to see more Zero-Knowledge Proofs as a solution to see for these problems?

Microsoft couldn't sell ZKP-based solution because parties needed to know who the counterparty is.

Liquor-buying: Truage - NACS national association of convenience stores does pseudo-ZKP. They give you 10 temporary credentials then you present that in the convenience store when you purchase.

Predicate Proofs - e.g. birthday (in number form), the verifier initiates a computation which spits out a yes/no on the question of is this person over 18?

Selective Disclosure as a promising solution

How Cloud Wallet Could Act as a Bridge in the SSI Space

Session Convener: Mike Schwartz
Session Notes Taker:

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Mike shared some slides that he presented at a Web3 conference in 2022: https://docs.google.com/presentation/d/1tJt_PaKq9jLLP1L4bjvUjRhdPqZdi3aSCB4T-zPPK08/edit?usp=sharing

In the presentation, Mike described the impact of the change in trust model from :
Issuer -> Verifier (or IDP-SP in federated identity terms)
to
Issuer -> Holder -> Verifier

He pointed out that by changing the data flow dynamics from two parties to three parties, there was a material impact on the resulting trust requirements. For example, the Verifier now needs to trust **both** the Issuer and Verifier. One of the first real world examples of decentralized identity presentation is the acceptance of mobile driver's license to board a flight in the Arizona airport. Note in this case, the Verifier (the TSA), only trusts a license held in an Apple wallet. A conversation ensued: why should the TSA care what wallet holds the credential? After all, the wallet doesn't matter when we present a plastic driver's license. However, this analogy is misleading--the Apple wallet is actually a driver's license component, not merely it's container. Furthermore, the TSA trusts Apple to protect the citizen's private key. Obviously, allowing a person to board a plane requires a high level of assurance--the TSA's limited trust scope (AZ issued ID in Apple Wallet) is therefore appropriate in this case, and at least shows that it's possible.

One of the main risks of federated identity is the risk of deplatforming. After all a "cloud" id is not decentralized. But Mike asked if perhaps it might make sense to launch a cloud wallet as a stepping stone to decentralized identity. It would enable Verifiers to start building the next generation of services, without having to wait in lockstep for wallets to evolve. Perhaps cloud wallets in the future could enable export to non-custodial wallets, enabling people a need to hold their verifiable credentials locally. This is analogous to FIDO tokens. Maybe people will choose to use "passkeys", which are FIDO tokens stored in the cloud (e.g. Apple backs up passkeys to the iCloud keychain); people who don't want Apple to store their private keys can use USB tokens, which have non-exportable private keys.

Mike also raised some questions about the maturity of decentralized credentials. For example, the W3C has not taken on all aspects of verifiable credentials, for example presentation or revocation. And there is likely to be a diversity of credential formats. EIDAS will use x.509, motor vehicle regulators are likely to use ISO mDL, and several other formats exist, like AnonCreds, VC-JWT, and LD Proofs with BBW+.

Finally, it's not clear how end-users will use digital wallets. In the payment space, Apple and Google wallets are popular. In the ethereum space, Metamask is popular. Some governments are building wallets (like the EUDI Wallet). And of course the Linux Foundation has raised millions to catalyze the Open Wallet Foundation open source project. It's not clear which wallets will emerge in the future, or what is the security profile for credentials presented via these wallets.

Another plus for Cloud Wallets is the development of OpenID for Verifiable Credentials: https://openid.net/openid4vc/ These draft specs provide a clear vision for how websites could use verifiable credentials originating from a cloud wallet.

To summarise, despite the palpable excitement around decentralized identity, adoption of the technology may take longer then expected--probably at least 10 years or more. It is likely to form an important building block of the future digital society. But it's hard to say if it will be our digital society, or that of our kids or grandkids.

See also Mike's blogs:

https://gluu.org/decentralized-identity-part-1/
https://gluu.org/decentralized-identity-part-two/
https://gluu.org/decentralized-id-part-3-credential-and-did-methods/

DCDR - Data-Centric Digital Rights (DCDR) Framework

Session Convener: Jean F. Queralt
Session Notes Taker: Merul Dhiman
(optional) List of Session Attendees:
Ashish Tripathi - Merul Dhiman - Kim Geun-Hyung - Deng Silorio - Carmen Lam - Others

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Problem Statement:
Policy makers and compliance regulatory agencies have published laws and provisions on how to protect data or data rights but without a corresponding technical documentation or better, an algorithm to guide coders/ programmers when developing/building their own applications. Hence and however, programmers/coders for that matter may have a different view or interpretation of the law, policy or such published regulation.

How to translate sense of purpose in technical terms for the digital ecosystem - Digital centric digital rights.

Discussion of Concepts:
Two things common for any individual are birth and death. Everyone strives to extend the gap between birth and death.

Data is you and yourself.

For digital data, the life cycle span is between two points: genesis and destruction.

- Data life cycle: data transformation then figure out when the destruction happens and when to avoid it to happen

Three (3) principles to navigate within the wireframe

1. i am my data
    - to treat someone else's data as yours
2. end remedy, remedial compensation
3. rights by design - do not leave any right uncoded
    - any single right should be transparent

Data operations are : CRUD and notifications.

Additional notes:

- Quality of data date depends on its accuracy and agency
    - accuracy is how well the data being collected and applied can describe you in a particular context or use case
    - agency is how much control or management a person has over the data
- GDPR or Data Privacy Act/Law should be supplemented by SDKs
- Data on its own is not useful. The algorithms make data useful (or harmful)

- Principles
    - Coders treat other people's data as their own
    - No remedy
    - Rights by design

ARE THERE NEXT STEPS as a RESULT of THIS SESSION?

- Will you take any Next Steps and/or continue this conversation? **YES**
- If so, can others from the APAC unConference join? **YES**
- If YES, please provide Contact Information for those who are interested:

  Jean F. Queralt: JFQueralt@TheIOFoundation.org
  DCDR Framework W3C Community Group: https://TIOF.Click/DCDRW3CJoin
  Current DCDR Framework documentation: https://TIOF.Click/DCDRDocs

SESSION #5

Open Discussion - Singpass - Singapore's National Digital ID

Session Convener: Yee Noi Lim
Session Notes Taker: Tze Yuan Lee

Please list the key points of your conversation and/or what you would like to share with your colleagues.

1. History of Singpass in Singapore. It started as a set of user ID and passwords.
2. 2FA was introduced using one time password was a step up credential
3. Singpass app was created as a method to issue crypto proof if an individual's digital identity.
4. The Singpass suite of API is build on the OIDC and OAuth open standards.
5. Physical card or digital ID is the primary? Singapore was fortunate enough to have a national registration act as a foundational ID
6. Smart phones, feature phones, different non app based options were launched in India to solve inclusivity problem
7. What were some of the challenges to onboard relying parties in the ecosystem?
    1. Small teams who does not have a technical development team
    1. Ask if Singpass provides funding and unfortunately Singpass does not
    1. Do not even have a login system misconception that Singpass is a primary login system and it is not
8. On charging, there is a "freemium" tiered pricing structure to encourage adoption, and then charging based on a cost recovery principle.

2D "Not QR" Codes + Civil Registration + Vital Statistics

Session Convener: Eric Welton (Korsimoro)
Session Notes Taker:

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Emergency Situations

- Identity Platform
- Reproducibility of barcodes vs device-driven verification
- Enroll digitally your medical records before doing scuba diving
- Tag a wallet as a special wallet (for emergencies)
- IKEA - 2D barcodes
- Cryptographs - card that has

General fear as putting biometrics in QR code.

What are the real risks of having PII in a 2D barcode? The data should have the personal photo.

It doesn't work really well with people crossing borders.

From one side: it's a great idea to have basic information but not including

How do you make this data secure?

How do you make sure that this data is not leaking? Just the simple storage

Krygystan - 5 government offices were robbed; hard drives containing biometric information were stolen.

What did they do with the data? Not sure. There have been an increase in the number of scams in recent years.

Having a central database of raw images is very risky. Government has to do it.

What risks are there at the personal level in having these information in a barcode/cryptograph?

The photo template is not the image itself. The app will encode the picture, send it to the verification server, come up with the template then compare it. You can't go from a template and get the raw image.

There are solutions that doesn't require a verification server.

The card has: image template, Verifiable Credential + PII

What is the effort needed to steal?

- Math formula to create the template
- Get the raw image

The cost is too much to attack. There is an opportunity of attack in an offline context.

- Danger Window - how long do we allow a VC to be verified offline

Physical Credential

- Passport image has latent data in the background which is revealed when you look at it with a different wavelength.

Revocation?

- Real-time has to be online and can't be offline
- A possible solution would be having a validity period (e.g. has to be refreshed every month)
- ZK-based verification at the wallet level
- There is no system that makes that "danger window" to zero

Public Key Infrastructure (PKI) Server would cost millions. Hardware Security Module (HSM). CA would take 2-3 years just to be approved on the global level.

Digital Signatures with other governments would need to go through PKI.

How many people would really need digital signature use-cases? Individual will have to bring their own key if they need that specific usecase.

Companies will also have their own verifiable credential. Verified Legal Entity Identifier.

Environmental systems should have identity. E.g. rivers Is this possible in SSI?

The ecosystem itself increasingly have rights (e.g. US).

Dams that produce carbon certificates for the power produced. Trees have carbon credits.

How do you link a digital certificate to a thing? e.g. gem, pants. Is it important to do so?

Hospital - Operating rooms would need to track items in the room (e.g. dirty linens, etc.)

Identity is given to the smallest thing. In the case of rivers, it would be the plants and the fishes.

Facial Biometrics in Livestock - tracking; protecting the Angus brand

Tigers - conservation

Angus Brand Protection: They track the meat but punish the actors

Dasun Hegoda 👨‍💻 Retweeted

Gluu
@GluuFederation

Dasun Hegoda presents the Modular Open Source Identity Platform (MOSIP) based identity architecture of Sri Lanka at the first event APAC Digital Identity unConference #openid

9:11 PM · Mar 1, 2023 · **101** Views

Notes Day 2 / Friday March 3 / Sessions 6 - 10

SESSION #6

(ToIP) Digital Trust Ecosystems - Components, Mental Model - Looking for Feedback

Session Convener: Eric Drury
Session Notes Taker: Merul
(optional) List of Session Attendees:

Please list the key points of your conversation and/or what you would like to share with your colleagues.

- ToIP is working to establish digital trust
- Have gotten very far with technology but there is still a lot of missing areas with governance side of it
- digital trust ecosystem is defined by trinh's definition
- interconnected community of diverse institutional and individual participants in a trust architecture (combination of governance and human actors) in a trust environment
- Trust doesn't exist without any context
- [context] - { Trust Architecture } - [trust application]
- trust architecture ((governance, DIDs, data) -> Trust Registry -> Verifiable Credentials)
- context (use case, regulations, laws, acts, scope)
- not trying to develop new governance but leverage existing models and establish accountability by the presence of verifiable actors

SESSION #7

Identity and Domain Names

Session Convener: Gihan Dias
Session Notes Taker: Jean F. Quéralt

Please list the key points of your conversation and/or what you would like to share with your colleagues.

What are the dimensions of an identifier
DNS for personal identifiers
ACANN working group on DIDs, etc.
APTLD - Asia-Pacific TLD Association - working group
DNS-based permissions
indexing service is needed (as DNS does not have a search function)

presentation:
https://cloud.domains.lk/index.php/s/MZ3rWqEwKJZTGad

Relationships
Permissions
ICANN group

As a Newbie (weather technical or non-technical) What are the ways I can engage to be able to implement SSI?

Session Convener: Rys
Session Notes Taker: JP

Please list the key points of your conversation and/or what you would like to share with your colleagues.

"Do you really need the solution?" — Mike

Reasons you might implement SSI:

- Avoid getting "deplatformed"
    - Rules are "white and black"
    - "Terms of Adhesion"
- Not sacrificing privacy.
- Offline access

SSI

- Is not new (e.g. Credit cards)
- Does not need to be in blockchain
- Actors:
    - Issuer
    - Holder -- Right to data, Consent
    - Verifier
- Challenges:
    - Revocation

Case of Prescribed technology

- Limits innovation

Prioritisation:

- Work with stuff with greater impact
- Work on limited resources
- Productivity (e.g. Tool for blockchain vs Database)
- Lack of context between user vs devs
- Usability vs "Production grade" apps
- Language translation
    - Regional language vs unicode (potential to harmful content unsupervised)

Use Case (Ukraine Degree validation):

- Ukrainian universities cannot provide certification for refugees
- IOTA
- Prescribed by UNESCO
- Alternative
    - Remote DB

Use case (Human trafficking)

- Enrollment for fishermen — Biometrics
- Requires will by port owners
- Not sexy but works

Use case (Singpass / Aadhaar)

- Centralised
- Accessible
- Cheap
- Traceable (?)

Others

- Is this solution looking for problems?
- Back to fundamentals on what we're trying to solve.

Whiteboard Session: Elements That Make APAC Trust Framework

Session Convener: Tze Yuan
Session Notes Taker: Kaliya
(optional) List of Session Attendees:
Kaliya, Kee Wee, Dasun, Min Khang, Ashish, Kumar, Eric D, Zico, Ujjwal, Geun-Hyung, Deng, Cho, Ajay, Andrew, Davin

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Links that are useful for everyone's reference

Outcome: H[**ere's the google doc that we will continue to build on when we create a ground up initiative of an APAC trust framework template**]

Why did you come to this session?

- Understand x-border trust - Interop
- Place to consider what matters
- work with something - learn about own region
- I build products with SSI for the EU and US I want to work on something in my own region.
- We are biggest manufacturing region in the world - how we track what is going on in our own region and also address unorganised trade.
- look at ECOTS (not sure I spent this right)
- India-Singapore UPI interop
- In other regions public private partnership formed to build governance/trust frameworks could it happen here.
- Asian Network what is the way - standards working group?
- Orgs exist to benefit from representation in this region.
- How governments can work with each other.

Outline of where we got to in the session.
Consideration Existing Structures

- eIDs today
- examples of public private partnership

Chapters

- Interoperability
- Standards
- Geopolitical/Cultural contexts of each country
    - Trust processes Pan Canadian Trust Framework

Framework lists for wallets

- Receive
- Hold
- Give

Considerations in the conversation

- Wallet Design - does the “trust” depend on the wallet
    - VCs are verified based on cryptography and pointers within them - don’t need to “trust” the wallet.
    - Wallet Security Working Group - to consider many issues
    - Wallet and or credentials anchored to hardware?
    - Tampered with vs. Confidentiality vs. Availability
    - Request flow vs. Verify

Use cases

- migration of worker
    - stakeholders - migrant workers, employers => proof of residency

Next Steps

- Potential home - Trust Over IP APAC Exploration Group
- Join the DIF/ToIP APAC monthly call.

Kaliya shared some of the history of eIDAS 1, middleware mess with 200 different schemes and eIDAS2 eIDAS Digital Identity Services in the Platform Economy

Pan-Canadian Trust Framework Overview PDF

Pan-Canadian Trust Framework - detailed PDFs

Private Sector Pan Canadian Trust Framework

US Government - Presentation about Green Cards

DHS USCIS Privacy SVIP Digital Credential

DIF Interop Protocol Landscape Diagram.

APEC Business Travel Card (ABTC)

Design Principles - Trust over IP

Regi-Trust

Digital TRUST Infrastructure for Discovery and Validation

"Agile Nations": Nations Sign First Agreement to Unlock Potential of Emerging Tech
Agile Nations Charter

Trust Registry Protocol Specification

Trust REgistries Drafting Group Meeting Page

EU TRAIN -

x509 DID registry alignment

ARE THERE NEXT STEPS as a RESULT of THIS SESSION?

- **Will you take any Next Steps and/or continue this conversation? YES**
- If so, can others from the APAC unConference join? **YES**
- If YES, please provide Contact Information for those who are interested:

Tze Yuan Lee: tzeyuan.lee@assurity.sg

SESSION #8

Building Open Source Communities + New Ideas

Session Convener: Mike and Dhaval
Session Notes Taker:

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Dhaval Slides: https://shorturl.at/yLQX2
Mike Slides: https://gluu.co/con-2023

Develop community from ground up (Dhaval):

- Open source project needs to ensure it has basic necessities to building and host a community from ground up
    - Document for adopters and contributors. For example, adopters need documents like 'Installation Guide', and when they try to contribute to the project, they need documents like 'IDE workspace setup guide'. Such documentation should ease the entry into the ecosystem.
    - put in place smooth contribution flow with necessary automation. For example, automate assignment of PR reviewers using GitHub 'codeowners' so that contributors don't have to find out who is supposed to review the PR.
    - Leverage automation to create quick feedback loops. For example, integrate static code analysis with PR creation so that contributor and reviewers are aware of issues in the submitted code.
- Different types of community participants that we have seen. Adopters, organisations, domain experts, technologists.
- Maintain the community and their engagement by continuously monitoring the health (tools: https://chaoss.community/ and https://devstats.cncf.io/).
- Keep the community engaged using processes like continuous triage. Use open communication channels to bring transparency.

New ideas (Michael):

- Different types of OSS
    - Volunteer Driven
    - Coopetition
    - Pure Play
- Lack of monitory rewards and support for volunteer driven OSS
- Discussion on how coopetition model works
- Discussion on Pure play OSS and Open core model
- Define and demystify - Web3 - and cryptocurrency is not the only use-case but only one of the use-cases
- Significance of token as a bond and how it can be leveraged

- How DAO(Decentralized Autonomous Organisation) works and leverages token based rewards
- Core open source project: Inception, Interaction with core team, community and paying customers
- DAOs can help remove startups as payment interdiatories and enable businesses and end beneficiaries of OSS to directly reward the core team and the community
- Challenges before successful DAO
    - Governance
    - Security

Social Media - "The Bali Process" Context: Human Trafficking Transnational Crime

Session Convener: Eric Drury
Session Notes Taker: Kalyan Kulkarni, Merul
(optional) List of Session Attendees: Eric W, Lana (Svetlana), Kalyan, Eric, Pru, Simran, Rys, Merul, Victor, SongJun, Ashish, Jacques von B, Ujjal D, Ashish, Nhi Bui

Please list the key points of your conversation and/or what you would like to share with your colleagues.

This is about human trafficking in the region. Following two issues to deal with and brainstorm on in this session

1. Verified on Twitter or something similar means nothing
2. Scams - Huge problem - people get scammed online

Where does Digital Identity come in? How can we educate the people on Digital Identity, sensitise them on the rights.
What should be the 5 to 10 points we should emphasize to them?

Victor stated that the second problem is more complex and complicated.

Pru & Eric W - Ad Technology being used deliberately to offer/get support for escaping

Svetlana - Education is the key. I never looked at LinkedIn as a professional tool but it was more a social media tool.
Victor - Maybe the refugee does not want to be identified.

Ashish - The way we have User onboarding journey documentation, we should build similarly, stories for the refugees to educate them

- The Bali Process: forum for policy dialogue and information sharing to combat the human trafficking problems
- Mostly human trafficking is coordinated via social media, actors impersonate someone who they are not, entice the targets by luring them into a job or propose having a relationship and then eventually trafficking them
- The current verified tick mark means absolutely nothing in the current scenario
- Facebook is the only one being in the slightest way being more rigorous
- Scams on social media are also quite prevalent
- Where exactly does DID come in and solve the whole problem
- Where can the people go to the stakeholders in order to push for the solutions

Our Journey to SSI in Thailand (use cases & poc Call for Collaboration) / Finema

Session Convener: Catherine
Session Notes Taker: Catherine

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Finema is an Enterprise Decentralized Identity solution provider.
Over 6 years old now with a proven track record of selling Digital Identity solutions to the Thailand Government.

Approach

- Top to Bottom Approach: Finema started off by educating the Thai Government about SSI for close to 3 years
- Once the Government is receptive, it is easier to push the Technology to the end users.
- There is a recommendation about the W3C Verifiable Credential Data Model translated in Thai that the Government agencies use as a reference.

Use Cases include:

- Thailand Pass which was a vaccine certificate verification platform that was used to verify all the vaccine certificates of everyone entering Thailand during the covid period. This was a breakthrough as the Government became more receptive to Decentralized Identity and it has led to other projects such as
- Digital Certificates
- Medical Certificates in the form of a verifiable credential that will be exchanged with the insurance companies to ascertain claims.

Call for Collaboration-Project based with anyone in the space. (QR code below)

SESSION #9

Blue Economy and Regional paperless trade / Eric W

Session Convener: Eric W
Session Notes Taker: Kalyan Kulkarni
(optional) List of Session Attendees: Jacques von Benecke (DHI), Svetlana, Catherine Nabbala (Finama), Andrew, Ujjwal D (DHI), Nhai Bui, Kalyan Kulkarni (AyanWorks), Eric Drury, Daven (Gluu)

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Eric W - There is a "Paperless Trade" initiative taken up by UNESCAP. One of the recent papers states that they are looking at leveraging DIDs & VCs for cross border trade. There is no clarity on the future roadmap or plan.

Jacques - Bhutan is bringing up a framework to use VCs for Issuers and Verifiers. Cross country trade is being discussed with the Swiss Govt. There is a lot of work we are bound to do with the central bank in Bhutan. The Central Bank is slow at the pace to bring innovation.

Eric - Does anyone know or want to speak about GLEIF.

Jacques - Described the GLEIF and the history about how that was brought up starting from the European union. LEI and VLEI (Verifiable LEI) both can be leveraged.

Kalyan - There has been effort to move in leveraging VCs for LEIF

Jacques - LEI can also have a level of hierarchy for delegation of authorities. Every issuer is verified before he gets a license issued to.

Eric W - Presented UN/CEFACT white paper draft by UN on Verifiable Credentials for Cross Border Trade.
https://unece.org/sites/default/files/2022-06/010_Verifiable-Credentials-CBT.pdf
https://unece.org/sites/default/files/2022-07/WhitePaper_VerifiableCredentials-CBT.pdf
https://tina.trade/app/dashboard

Eric W - Cananyone throw some light on how digital signatures are used in respective countries to sign the trade agreements as such.

Kalyan - In India, we do have authorities using their digital signatures being used by subordinates to sign on behalf of the authorities - not aware of the trade agreements in particular. We also have ink signatures used.

Ujjwal - We ask for power of attorney for someone to sign the documents. There are gazetted officers who are designated to sign specific documents.
Kalyan - India has an eSign (Digital Signature) and eSeal being put on each govt issued documents. We have seen resistance by the govt officials to bring VCs as a new norm in spite of the benefits it poses in the long run.

Eric D - Important part to it is - if Asian country has a trade interest with Europe, then it makes more sense for them to establish the paperless trade.

Share the Journey of IAM Delivery Work - do's don'ts Lessons Best Practices

Session Convener: Dave Yip
Session Notes Taker:

Please list the key points of your conversation and/or what you would like to share with your colleagues.

I didn't prepare well for the session which I apologized for. I would like to share my experiences in my 20 years of IAM delivery work but due to the lack of preparation, I missed mentioning many useful points during the session.

However, the session went quite well with the help of Mike.

We talked about the following IAM delivery tips:

1. Top executive support is critical to have successful IAM solution implementation.
2. Good stakeholder communication and seek stakeholders involvement as early as possible.
3. Focusing on whats matters and avoid scope creep. Delivery small and get quick win instead of adding too many requirements and make the project too difficult.
4. Have proper identity data cleansing done before the system goes to production.
5. Drive the project with industry best practices. Alert the customer loud and clear with written communication if the customer wants something that will lead to future issues.
6. Ensure the system will run and be operated smoothly in production by having vigorous load/perforamnce tests and operational tests.
7. Have an independent expert to review the the design to ensure the proposed architecture adheres to best practices and can handle real production loads.

ARE THERE NEXT STEPS as a RESULT of THIS SESSION? YES!

- Will you take any Next Steps and/or continue this conversation? Yes
- If so, can others from the APAC unConference join? yes
- If YES, please provide Contact Information for those who are interested:
    - sy.yip@gamatech.com.hk
    - +852 63034001

Analyzing Structured Data's LIfe Cycle

Session Convener: Jean F. Queralt
Session Notes Taker: Notes entered by convener post-session
(optional) List of Session Attendees:
Ashish Tripathi, Merul Dhiman, Kim Geun-Hyung, Others

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Problem Statement:
Building on Day 1's session (DCDR - Data-Centric Digital Rights (DCDR) Framework -Day 1 / Session 4 / Space E), the session focused on analyzing the life cycle that structure data goes through with the intention to infer what are the damages it can undergo, thus categorizing them as "Harms".

Discussion of Concepts:
The session discussed topics on:

- What does the life cycle of structured data look like?
- How can it be represented in a proper diagram?
- What are the dimensions that correlate a Source Entity (physical world) with its Representational Entity (Digital Twin)?
    - Authenticity
    - Accuracy
    - Agency
- What are the different options for "data demise"?
- What is the general diagram for data exchange?
    - Signals / Messages
        - Request
        - Reply
    - Notifications
- If the elemental operations are CRUD, what could be considered as data-transformation primitives?

ARE THERE NEXT STEPS as a RESULT of THIS SESSION?

- Will you take any Next Steps and/or continue this conversation? **YES** / NO
- If so, can others from the APAC unConference join? **YES**
- If YES, please provide Contact Information for those who are interested:

Jean F. Queralt: JFQueralt@TheIOFoundation.org
DCDR Framework W3C Community Group: https://TIOF.Click/DCDRW3CJoin
Current DCDR Framework documentation: https://TIOF.Click/DCDRDocs

Image Below

(Zoomed in shots of this are available)

SESSION #10

NFTs as an Identifier - Pro's Con's Is it worth it? NFT adoption and applications

Session Convener: Mike - Victor
Session Notes Taker:

Please list the key points of your conversation and/or what you would like to share with your colleagues.

It's helpful to review the basics. What is an NFT?

NFT's are defined by ERC-721:

Interfaces:

```
interface ERC721 /* is ERC165 */ {
    event Transfer(address indexed _from, address indexed _to, uint256 indexed _tokenId);
    event Approval(address indexed _owner, address indexed _approved, uint256 indexed _tokenId);
    event ApprovalForAll(address indexed _owner, address indexed _operator, bool _approved);
    function balanceOf(address _owner) external view returns (uint256);
    function ownerOf(uint256 _tokenId) external view returns (address);
    function safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes data) external payable;
    function safeTransferFrom(address _from, address _to, uint256 _tokenId) external payable;
    function transferFrom(address _from, address _to, uint256 _tokenId) external payable;
    function approve(address _approved, uint256 _tokenId) external payable;
    function setApprovalForAll(address _operator, bool _approved) external;
    function getApproved(uint256 _tokenId) external view returns (address);
    function isApprovedForAll(address _owner, address _operator) external view returns (bool);
}

interface ERC165 {
    function supportsInterface(bytes4 interfaceID) external view returns (bool);
}

interface ERC721TokenReceiver {
    function onERC721Received(address _operator, address _from, uint256 _tokenId, bytes _data) external
}
```

Schema:

```
{
    "title": "Asset Metadata",
    "type": "object",
    "properties": {
```

```
    "name": {
      "type": "string",
      "description": "Identifies the asset to which this NFT represents"
    },
    "description": {
      "type": "string",
      "description": "Describes the asset to which this NFT represents"
    },
    "image": {
      "type": "string",
      "description": "A URI pointing to a resource with mime type image/* representing the asset to which this NFT represents. Consider making any images at a width between 320 and 1080 pixels and aspect ratio between 1.91:1 and 4:5 inclusive."
    }
  }
}
```

It's important to remember that NFT's are not "held" in a wallet. A digital wallet (like Metamask) really only holds the keys, which enables it to prove control of an asset referenced on the Ethereum blockchain.

Thus, NFT's are a pretty interesting container, in which you can implement all kinds of solutions. OpenSea implemented an ecosystem based on the trading of rights for digital images. However, other ecosystems are possible. Identity architects could use the metadata claims "name", "description" and "image" for all sort of interesting applications.

It is possible to make an NFT non-transferable by returning null in the transfer interfaces. For example, a POAP (Proof of Attendance Protocol) is a protocol used to verify and authenticate physical attendance at events. It gives event organisers the ability to issue digital badges and certificates to participants that are secured with blockchain technology, allowing them to prove their attendance at an event. POAPS are NFTs--normally the attendee scans a QR code from a poster which transfers the POAP to the attendee's Matamask wallet. Non-transferrable NFTs can make sense for certain identity ecosystems. For example, for digital driver licences, if you lose it, you have to re-enroll (and get remote identity proofed again… which maintains the same level of trust in the credential). Health ecosystems also require re-identity proofing to recover your credential.

It is important to remember that the Ethereum blockchain is public, so privacy considerations ensue. You cannot store even encrypted PII on the blockchain, which is why the storage of one-time hashes and other ZT proofs is becoming prevalent for public data. This offers the benefits of the tamper-resistance and distribution features of blockchain.

However, sometimes people want to make their information public. In their web3 ecosystem, Tea.XYZ is issuing NFT's to package maintainers (i.e. think NPM or Linux package repo) for reputation and rewards (also loss of rewards as penalty for delayed security fixes). This is an interesting use case which has actual utility, and shows the flexibility of NFT applications.

Open Source Underdogs Podcast:
Tokenizing the FOSS Package Ecosystem, with Max Howell, Founder of Tea.xyz
https://opensourceunderdogs.com/episode-57-max-howell-founder-tea-xyz/

Victor talked about the application of NFT's in the gaming sector, enabling transfer and interoperability. Perhaps you get to level 10 in a game, and you want to sell that progress to someone else (who doesn't want to waste the time getting to level 10…). NFTs make a lot of sense for trading card games too. While anonymity is common, digital identity can enhance the value of gaming ecosystems. Reputation is also important.

One final point was raised: there is a saying that adoption is more important then standards. NFTs are a general interest technology, that has captivated the imagination of artists and business people. Despite some of the early NFT tulip-mania, it is clear that NFTs are a serious technology. There is already significant amount of tooling available for NFTs. This make it an interesting technology on which to build part of an identity ecosystem.

Verifiable Credentials - Exchange Protocol and Wallet Interaction

Session Convener: Ashish T
Session Notes Taker:

Please list the key points of your conversation and/or what you would like to share with your colleagues.

Some tutorial around VC-API : https://w3c-ccg.github.io/vc-api/
https://github.com/energywebfoundation/ssi/tree/develop/apps/vc-api/docs
https://vc-api-dev.energyweb.org/api/#/

== From Rys

1. Requester → Application
2. You → Your are the data
3. You were issued data

Privacy
Consent
Control
Interoperability
Issuer, Holder, Verifier
DID → in blockchain-based solutions: did:etc:ews:address
did: did identifier
etc: method (create, read, update, delete)
ews: chain ID?
address: wallet address
DIDWEB → Domain
Similar to URI

Issuer: College
Holder: Student
Verifier: Employer

1. Student requests College to issue credential
2. College will issue VC
3. VC is held in Student Wallet
4. Employer requests Verifiable Presentation Request (VPR)
    1. Employer System: Initiate Exchange (exchange ID)
    2. Wallet: Acknowledge the request
    3. Employer System: Send VPR
    4. Wallet: VP
5. Student approves VPR, wallet returns a VP
    1. Subject: DID
    2. Metadata
    3. Proof: Issuer DID
6. Employer System can verify VP via Proof field

Authentication

1. You use the DID to sign a “payload” (e.g. session) which gives out a signature
2. From signature: payload & DID can be derived (using public and private key infrastructure)
3. The signature goes back to the authenticating system and verify the signature

The “act” of signing, how does it happen? Is it clicking a button?
→ Depends on the user interface
→ In non-blockchain systems (e.g. hardware systems)
→ In blockchain systems on the web where there’s a wallet (e.g. Metamask), this is an interface that shows you what you’re signing, then there’s a button to “sign”
→ There can be an extra layer of security (e.g. SOA challenge)

Verifiable Credential API

Spec from W3C, Configurable

https://w3c-ccg.github.io/vc-api

https://github.com/energywebfoundation/ssi/

Attendee Comments on Participating in the APAC Digital Identity Open Space unConference

At the end of each day we provided a few minutes for participants to reflect on their experience and to complete the sentence:

"As a result of attending the APAC Digital Identity UnConference…."

- *I've made valuable connections from the APAC region that will help continue to explore more equitable and dignified ways of implementing DID systems. We are leaders in this space and have the power to influence thinking around how we shape Asia's identity space.*
- *I got to network with a lot of wonderful people and explore various philosophical, logistical, logical and technological aspects of SSI.*
- *I go back with a newer perspective, I learned so much, and found new areas to explore.*
- *I got to experience exactly what an Open Space unConference is, meet awesome people and networking, understanding the process of transforming the foundation identity to the digital.*
- *I will regard identity as a right that is given to the individual not the tool of a government.*
- *I received a tremendous amount of insights into the SSI space, business ideas, use cases, and models to help adoption. Very happy with the connections made.*
- *My first time attending an unConference, thanks for interesting discussions. It is a pleasure to meet everyone!*
- *Same minded human beings with a promise to solve issues on identity which is important to all citizens for an open transparent society.*

- *I am able to find brilliant minds and resources to help me, my team and my country more to a better state and focus on the solution.*

- *It is vitally important to raise public awareness about issues related to digital ID so that they can not only become smart users/owners but also contribute to make a safer digital world.*

- *I know I have a lot to contribute and look forward to. Let's roll it!*

- *I learned how to make sure I use technology to solve a problem, and not find a problem to test my technology.*

- *Made some valuable connections and got to know who is doing what in the space.*

- *Everything I experienced here came new and precious. I want to thank all the staff members.*

- *I understand what is on the horizon for identity space, and got to know lots of interesting use cases. Loved the Open Space unConference format.*

- *I got to meet a diverse set of audience all working towards the larger goal of digital ID and decentralized ID. Wonderful format of the conference that I would like to try out at other events.*

- *I learned more about Identity and technology such as NFT, Trust Registry, how to market products etc…*

- *I get to know where national identity implementation is in the ASIA regions.*

- *Great learning experience from passionate people. In some aspects an eye-opener for projects I was aware of but never had the opportunity to learn more about before.*

- *I feel this is the beginning of a beautiful friendship…*

- *…I have renewed and revitalized confidence in our tech for social/regional change.*

- *The exposure and different perspectives of the digital ID domain is really important and valuable and I hope to be connected to contribute and collaborate.*

- *I see regional leaders (individuals) emerging in the digital identity space.*

- *I see lots of interest to remain connected and exchange conversations. The quick action of forming a Trust Registry - APAC is great! Just like the IIW, people here are doers. Lots of hopes for the next one.*

- *I have made new friends and gained much from the sharing of everyone. Thank you to the organizers and all the attendees. I hope that the sharing I did was helpful to some of you at least. Cheers and keep in touch. Leaving with a full tummy and full brain of ideas to digest….*

- *I'm happy to attend the meeting about the new approach and ideas about the tech. I want to share it with my team in my own country. I can get new valuable experience and by leveraging it, I want to deep dive more and more.*

- *I have gained more perspective on challenges and opportunities. Met and made connections with some very smart and passionate experts. Really found the event valuable.*

- *I've learned about Digital Identity as a technology and ideology. I've realized the infrastructure that we're in the Philippines to get to a proper Digital ID economy.*

- *I've increased my appreciation for a flexible conference format. I've substantially broadened my understanding of existing projects being implemented in the APAC region.*

- *It was great meeting everyone in the conference, especially those that I can put a face to after conversing over email and tickets (shout out to Gluu & Goutech) . It was great to know the direction that is heading in the APAC region. I hope to get in touch more and learn more.*

- *I am extremely happy and honored to meet many new/old friends in the digital ID space. And learn new perspectives from many.*

- *I think we explored what it means to be collaborative in this conference. I hope we can keep momentum going and build a better trusted world.*

- *I gained new knowledge, met likeminded people, explored more in the digitalID space which allowed to evolve and deliver better services*

- *Really interesting unconventional approach towards ID and Privacy. Loved the model of the discussion's presentation.*

- *First time attending this type of meeting, very interesting and I learned terms I didn't know. Next time, I wish to speak.*

- *Met a diverse group of people, I learned the MOSIP is not known much, interesting viewpoints around SSI*

- *My understanding of Digital Identity is better and the various use cases that are presently used.*

- *I know that I can get first hand insights from experiences of others and contribute myself in such forums*

- *I understand more about the challenges faced in implementing SSI and or verifiable credentials*

- *I had a valuable time to learn many issues related to self sovereign identity and data privacy. WOW!!!*

- *I realized that Identity is an integral part of many systems and should not be an isolated discussion on its own*

- *I got to learn about various identity initiatives in different countries. I met people from different countries, giving me the opportunity to know about various identity initiatives they are undertaking. The sessions were really interesting and wonderful.*

- *I met many likeminded people in the digital identity space in the APAC region. It's a great thriving community.*

- *I learned how big of an impact political will has in driving adoption of these foundational systems. I've learned to also consider non-typical use cases and really think about tech impact in people's lives.*

- *I love it. Got the wisdom of transforming the foundation identity to digital identity. Knowing and meeting awesome people here.*

- *The technology is there, it's really the policies, the initiative, that needs to be fleshed out.*

- *I learned about new ideas, tools and mostly new perspectives towards problems in the identity space. Hope to collaborate more with people and contribute to the space more.*

- *The interest in cross border identity and challenges for implementation.*

- *I know a lot more about DID and SSI use cases and also know governments are rolling out identity infrastructure.*

- *I realized that the countries in the APAC region are getting on the new edge/ age of Digital Identity and hence have opportunity/need to collaborate.*
- *I have more knowledge about digital identity and its connection to many aspects of life.*
- *Met many people of APAC and learned the different viewpoints of how we can approach and use digital identity*
- *I am able to take my research one step further.*
- *I have more confidence to move forward with my startup project.*
- *I learned that I have so much more to learn and have so much more to share. Out of the box scenarios are worth exploring because they aren't just edge cases.*
- *Extensive coverage of APAC region in terms of representatives*

Photos From Day 1

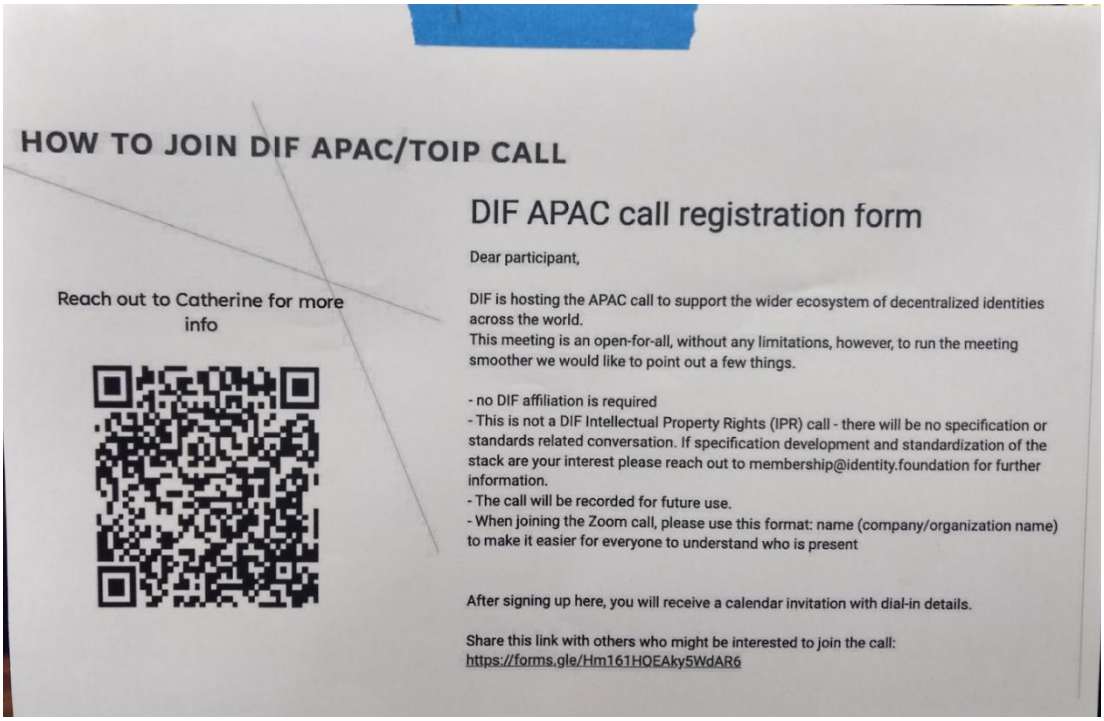
Participants in these photos consented to having their images shared.

Please find HERE a selection of photos from Day 1 of the unConference

Stay Connected with the Community

Join the Monthly DIF APAC / ToIP Call

How to Join the
DIF APAC / TOIP Call
https://identity.foundation/SIG-APAC/



Creating an APAC Trust Framework

Coming out of Session 7D/ Whiteboard Session: Elements That Make APAC Trust Framework / TY If you are interested in working on this please contact:
Tze Yuan Lee: tzeyuan.lee@assurity.sg

Building a Data-Centric Digital Rights (DCDR) Framework

Coming out of Session 4E / Data-Centric Digital Rights (DCDR) Framework **.** If you are interested in working on this please contact:

Jean F. Queralt: JFQueralt@TheIOFoundation.org
DCDR Framework W3C Community Group: https://TIOF.Click/DCDRW3CJoin
Current DCDR Framework documentation: https://TIOF.Click/DCDRDocs

APAC Digital Identity unConference 2024

The APAC Digital Identity unConference 2024 will take place in Bangkok, Thailand. Updates on its organisation should be available in the second quarter of this year and will be published on the event's page: https://www.apacdigitalid.org/en

If you wish to receive updates on the event in 2024 by email, please complete the **'Expression of interest: APAC Digital Identity unConference 2024'**form HERE.

If you have any questions regarding the event, please contact us at: contact@apacdigitalid.org

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