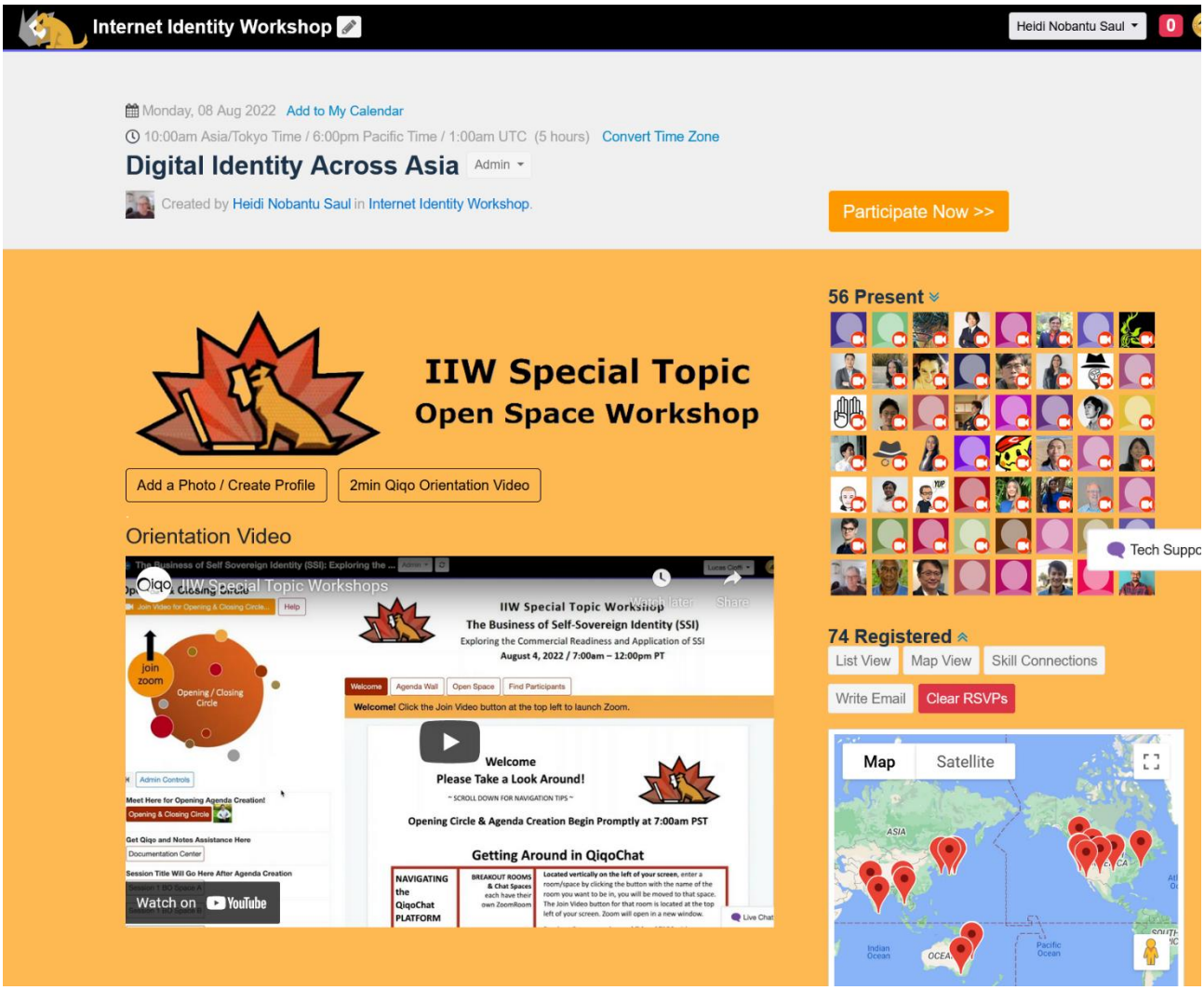
IIW Special Topic Workshop

Digital Identity Across Asia

Tuesday August 9, 2022

Book of Proceedings

Online, Near You ~ via [QiqoChat]

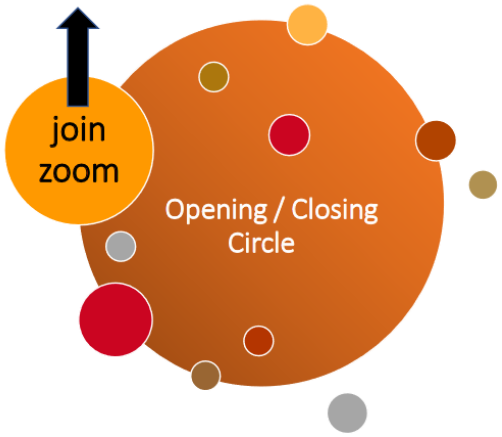


IIWXXXV is November 15 - 17, 2022 in Mountain View, CA

More information and **REGISTER HERE**

www.internetidentityworkshop.com

Contents



About IIW the Internet Identity Workshop

The Internet Identity Workshop (IIW) was founded in the fall of 2005 by Phil Windley, Doc Searls and Kaliya Young. It has been a leading space of innovation and collaboration amongst the diverse community working on user-centric identity.

It has been one of the most effective venues for promoting and developing Web-site independent identity systems like OpenID, OAuth, and Information Cards. Past IIW events have proven to be an effective tool for building community in the Internet identity space as well as to get actual work accomplished.

The event has a unique format – the agenda is created live each day of the event. This allows for the discussion of key issues, projects and a lot of interactive opportunities with key industry leaders that are in step with this fast-paced arena.

Watch this short documentary film: ***"Not Just Who They Say We Are: Claiming our Identity on the Internet"*** http://bit.ly/IIWMovie to learn about the work that has happened over the first 12 years at IIW.

The event is now in its 18th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young.

Upcoming IIW Events

IIWXXXV #35
November 15 - 17, 2022

Taking place in person at the Computer History Museum in Mountain View, CA

REGISTER HERE

\\\You can find the Book of Proceedings for previous IIW events here
https://internetidentityworkshop.com/

IIW Special Topic Event - Digital Identity Across Asia

Digital Identity Across Asia
Tuesday August 9th, 2022 / 1:00am - 6:00am UTC

IIW Digital Identity Across Asia Co-Hosts

- Kazue Sako / Waseda University/MyDataJapan / Japan
- Ms. Catherine Nabbala (Finema Co., Ltd) Thailand
- Sankarshan Mukhopadhyay / Public Interest Technologis / India

This IIW Special Topic event is for individuals, practitioners, researchers, regulators, technologists, digital and privacy rights activists. We encourage people interested in decentralized identity from around the globe to attend! It provides the space for you to discuss, share and collaborate together.

Digital Identity is complex - many different communities have been working on solutions for a long time. The Internet Identity Workshop has been convening for 17 years and was a key forum in the development of OpenID and OAuth widely used on the consumer internet and in enterprise systems today. In the last several years some new protocols have been developed by the community participating in the Credentials Community Group at the W3C, Trust over IP Foundation and Decentralized Identity Foundation among others.

This event continues the tradition of IIW creating 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.

Why this event is needed now, the themes we hope to cover and questions to answer ~

Significant investments have been made into the development of interoperable standards, protocols, systems application layers, conceptual use cases, and more.

These are important areas to be discussed in the region:

- readiness and maturity of the standards and components required to design, build, deploy and maintain a digital ID system for people at scale
- enabling digital ID systems which offer protection against surveillance and preserve privacy
- designing economically sustainable models for citizen services built around digital ID systems
- application of decentralized identity to the Internet of Things (IoT)

Who's the Event For?

- People who have been working on digital identity and Self-sovereign Identity (SSI) products and services
- Those new to the concepts of SSI and want to learn what it is all about
- Government leaders seeking to understand the technology
- Consumers of Self-Sovereign Identity (SSI) Products and services
- People around the world working on Decentralized ID

We encourage people interested in decentralized identity from around the globe to attend!

About The Format

We will co-create the agenda live the 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. We do know great people who will be there and it is the attendees who have a passion for learning and contributing to the event that will make it a success.

IIW Events are participatory workshops where the agenda is co-created by participants the day of the event. We are hosting half day Special Topic IIW events that are complementary to our main three day event that happens twice a year (since 2005!) using a similar format.

The workshop will run just like our usual IIW Open Space Workshops - with an Opening and Agenda Creation, 3 sessions and a Closing Circle, for a total of 5 hours. We will also have session notes and be compiling a Book of Proceedings.

The Internet Identity Workshop (IIW) has been bringing together innovators in the field of Identity focused around the individual since 2005. Please go to the IIW site www.internetidentityworkshop.com for additional information about the Internet Identity Workshop and to view the short video "What is IIW?"

Schedule - Tuesday August 9th

Time: Anchored in Asia TZ

- UTC 1:00am - 6:00am
- Delhi, India 6:30 am - 11:30am
- Bangkok, Thailand 8:00am - 1:00pm
- Tokyo, Japan10:00am - 3:00pm
- Melbourne, Australia 11:00am - 4pm
- Wellington, New Zealand 1:00:pm - 6:00pm
- Monday August 8th Pacific Time US: 6:00pm - 11:00pm

See the growing list of topics proposed by those already registered here: https://iiw.idcommons.net/Identity_Across_Asia_Proposed_Topics

IIW Digital Identity Across Asia Co-Hosts

- Kazue Sako / Waseda University/MyDataJapan / Japan
- Ms. Catherine Nabbala (Finema Co., Ltd) Thailand
- Sankarshan Mukhopadhyay / Public Interest Technologis / India

We look forward to seeing you virtually August 9, 2022!

Book of Proceedings is Sponsored by AyanWorks

Opening Circle Zoom Chat

19:02:01 From sankarshan mukhopadhyay to Everyone: This is exciting!

19:02:12 From John Phillips - Sezoo to Everyone: Nice to be at an online IIW event at a time when I'm meant to be awake! :)

19:02:40 From Catherine Nabbala to Everyone: Yeah! First ever IIW Asia 🙂

19:03:03 From Kazue Sako to Everyone: I see sun from my window!

19:03:27 From Tom Sato to Everyone: good morning. I am in Nagano Japan, today.

19:03:36 From Heidi Nobantu Saul to Everyone: Greetings from Santa Fe, New Mexico!

19:03:41 From John Phillips - Sezoo to Everyone: G'day from Melbourne - on a sunny winter's day

19:03:41 From James Schoening to Everyone: good late evening from New Jersey

19:03:43 From Kazue Sako to Everyone: I'm from Tokyo, Japan!

19:03:45 From Kosuke Koiwai1 to Everyone: Hello from Tokyo!

19:03:46 From Sammotic Switchyarn to Everyone Good morning from Bangkok!

19:03:46 From Jo Spencer - Sezoo to Everyone: Good morning from Sunn (but cold) Melbourne!

19:03:53 From Sagar Khole to Everyone: Good morning from India

19:03:54 From Dan Yamamoto to Everyone: Good morning from Yokohama, Japan

19:03:58 From Angelo Malundas to Everyone: Good morning! from Philippines

19:04:00 From Ken Watanabe to Everyone: Good morning from Tokyo, Japan

19:04:00 From Liem Truong to Everyone: Morning everyone! Joining from Melbourne

19:04:01 From Kento Goro to Everyone: Good morning from Japan

19:04:08 From Suneet Bendre to Everyone: Good Morning .. Pune (India)

19:04:08 From Catherine (Finema-Thailand) to Everyone: Hello from Bangkok, Thailand 🙂

19:04:09 From Ekta Zope to Everyone: Good Morning from India!

19:04:09 From Thomas Robin to Everyone: Good morning from a chilly Melbourne !

19:04:11 From Logan Porter to Everyone: Good afternoon from New Zealand!

19:04:14 From Kaliya Identity Woman to Everyone: Good Sunny evening from Oakland California!

19:04:20 From Kimberly (IIW Tech Host) to Everyone: Good evening from Cupertino, CA!

19:04:20 From Yuji Suga to Everyone: Yuji from Tokyo, Japan.

19:04:25 From sankarshan mukhopadhyay to Everyone: Good morning from Pune, India

19:04:31 From Munir Mohammed to Everyone: Good Morning from Bangalore India

19:04:43 From Nicole Khor to Everyone: Good morning from Gold Coast, Aus

19:04:51 From shinichiro matsuo to Everyone: Good morning from Washington DC, USA

19:04:56 From GeunHyung to Everyone: Good Morning from Busan Korea

19:06:02 From Kazue Sako to Everyone: Are we going to take a photo?

19:06:08 From Catherine (Finema-Thailand) to Everyone: we should

19:06:58 From Gihan Dias to Everyone: Good morning from Sri Lanka

19:09:09 From ericdrury to Everyone: Greetings from Bangkok!

19:09:27 From Catherine (Finema-Thailand) to Everyone: Hi Eric, good to see you

19:09:42 From ericdrury to Everyone: 🙂

19:22:33 From sankarshan mukhopadhyay to Everyone: If you'd like to tweet about and during the event - you can also tag https://twitter.com/idworkshop

19:32:44 From Mark Scott to Everyone: Good evening from Mapleton, Utah (normally San Diego, California).

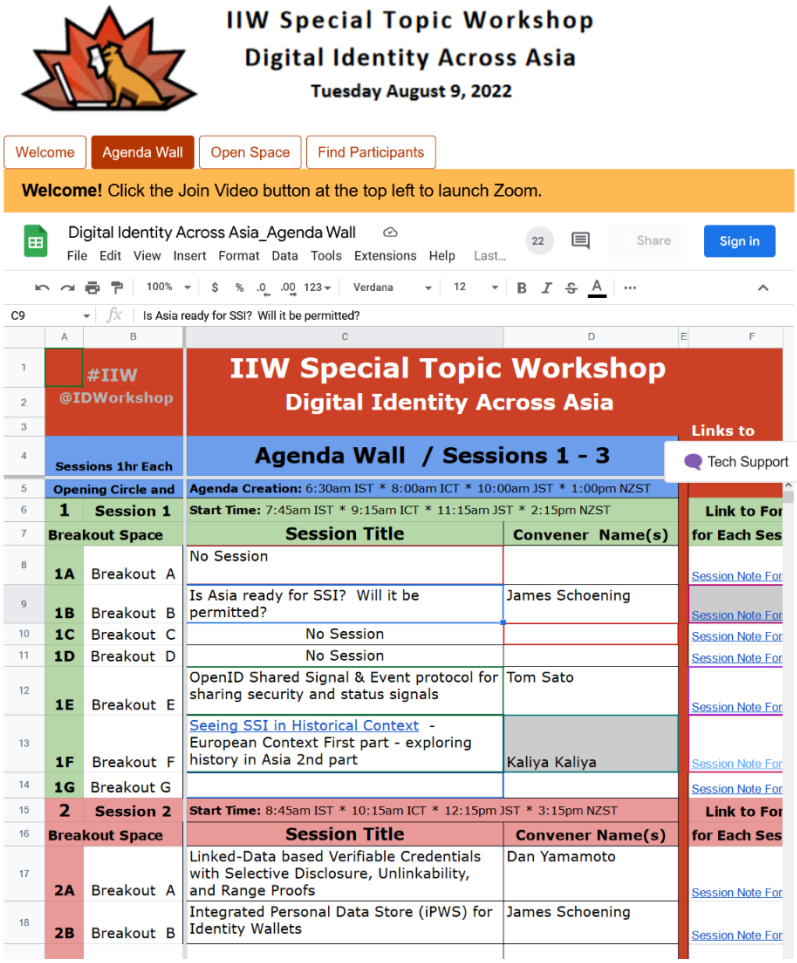
19:47:30 From John Phillips - Sezoo to Everyone: Always a pleasure to hear Heidi's introduction to the principles of open space 🙂. Delivered with passion and authenticity, these are powerful organising and empowering principles. 👏

19:48:00 From Kazue Sako to Everyone: +1 to John

19:50:32 From Eric Drury to Everyone: Thanks Heidi

19:51:33 From Kaliya Identity Woman to Everyone: Everyone is welcome to call sessions - on any topic 🙂

Session Topics / Agenda Creation



IIW Special Topic Workshop
Digital Identity Across Asia
Tuesday August 9, 2022

Welcome | Agenda Wall | Open Space | Find Participants

Welcome! Click the Join Video button at the top left to launch Zoom.

Digital Identity Across Asia_Agenda Wall

File Edit View Insert Format Data Tools Extensions Help Last...

Share | Sign in

C9 | Is Asia ready for SSI? Will it be permitted?

	A	B	C	D	E	F
1		#IIW @IDWorkshop	**IIW Special Topic Workshop** Digital Identity Across Asia			
2						
3						Links to
4		Sessions 1hr Each	**Agenda Wall / Sessions 1 - 3**			Tech Support
5		Opening Circle and	**Agenda Creation:** 6:30am IST * 8:00am ICT * 10:00am JST * 1:00pm NZST			
6	1	Session 1	**Start Time:** 7:45am IST * 9:15am ICT * 11:15am JST * 2:15pm NZST			Link to For
7		Breakout Space	**Session Title**	**Convener Name(s)**		for Each Ses
8	1A	Breakout A	No Session			Session Note For
9	1B	Breakout B	Is Asia ready for SSI? Will it be permitted?	James Schoening		Session Note For
10	1C	Breakout C	No Session			Session Note For
11	1D	Breakout D	No Session			Session Note For
12	1E	Breakout E	OpenID Shared Signal & Event protocol for sharing security and status signals	Tom Sato		Session Note For
13	1F	Breakout F	Seeing SSI in Historical Context - European Context First part - exploring history in Asia 2nd part	Kaliya Kaliya		Session Note For
14	1G	Breakout G				Session Note For
15	2	Session 2	**Start Time:** 8:45am IST * 10:15am ICT * 12:15pm JST * 3:15pm NZST			Link to For
16		Breakout Space	**Session Title**	**Convener Name(s)**		for Each Ses
17	2A	Breakout A	Linked-Data based Verifiable Credentials with Selective Disclosure, Unlinkability, and Range Proofs	Dan Yamamoto		Session Note For
18	2B	Breakout B	Integrated Personal Data Store (iPWS) for Identity Wallets	James Schoening		Session Note For

The Agenda of Sessions was co-created by attendees at the start of the workshop

11 Sessions were called and convened by over 70 participants

Notes were submitted for all sessions!

Session 1

1B/ Is Asia ready for SSI? Will it be permitted?
1E/ OpenID Shared Signal & Event protocol for sharing security and status signals
1F/ Seeing SSI in Historical Context - European Context First part - exploring history in Asia 2nd part

Session 2

2A/ Linked-Data based Verifiable Credentials with Selective Disclosure, Unlinkability, and Range Proofs
2B/ Integrated Personal Data Store (iPWS) for Identity Wallets
2E/ Building a community around privacy in India - Privacy Mode's approach and learnings.
2F/ Is SSI-on-blockchain objectively a bad thing?
2G/ All you wanted to discuss about Aadhaar

Session 3

3A/ Strategies for resisting vendor pressure on governments equating "digital-id = biometrics"
3B/ How organizations can make and save money with decentralized trust models
3C/ DIDComm for IoT Usecases

Session 1

Is Asia Ready for SSI? Will it be permitted?

Session Convener: James Schoening
Session Notes Taker: Paul Grehan

Tags / links to resources / technology discussed, related to this session:

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

Some topics :

- Cultural context in Asia - differences in region and with other regions in the world (Eric - Kosimoro)
- What's happening in the region in general
- Human rights are exceptionally underdeveloped after thought in general - what happens when we introduce identity tech (of any sort) to fundamental human rights?

Main theme :

If SSI goes viral - will some countries even permit citizens to establish sovereign identity and control their own data ?

- Development not represented, no ability to have requirements and needs expressed in technology solution
- this divide has not been well managed to date - does this technology exacerbate the issues that exist today

- t of SSI standards has cultural bias - are some cultures/countries not represented in current tech standards ?
    - Literacy barriers - digital literacy is an insurmountable task ?
    - Central regimes - pressures beyond the individual preventing adoption
    - shared burden for maintenance of data
    - context of identity is different, more community inclusive focus (Thailand)

Question? What if you are not included in mainstream society in the first place?

Danger of loss of individual freedom - what level of empowerment is available for the individual ?

Power imbalances impacting adoption of collaborative initiatives (ASEAN blocking advancement)

The convenor (James.schoening@ieee.org) provided his assessment, that the only viable path he can think of to spread SSI and online privacy to all is to try to gain adoption anywhere we can, to evolve the ecosystem and benefits, and then figure out how it can be spread to the rest of humanity, but those who have alternate strategies should pursue them too.

Additional NOTES:

[sankarshan]

I feel it is necessary to understand the existing patterns and politics around legal identity, large national digital ID projects and digital public goods powering citizen services in order to examine how SSI approaches align.

- What does the form of SSI mean in the various countries which are in this region?
- How does it help to grow some of the published initiatives from the government?
- What would a rights based digital identifier system look like from aspects of agency, control and protection from harms?
- Lastly, what gaps in the current design pattern of SSI would be surfaced when the technology approaches are adopted in these nations?

All these are critical to the wider adoption of a technology pattern.

[Lucy Yang]

It is important to understand how SSI has been developed until today. Kaliya Young's paper Seeing SSI Self-Sovereign Identity in the Historical Context explained how SSI emerged mainly under the influence of Western liberal values. However, this technology is positioned to fill in the gap of the missing identity layer of the Internet, which means it will need to serve a broader range of people than the group has worked to shape and influence it. Instead of asking the question of "Is Asia Ready for SSI", it is probably better to examine how we can make SSI suitable as a global standard/technology pattern for all to help different countries/societies address identity management issues.

OpenID Shared Signal & Event protocol for sharing security and status signals

Session Convener: Tom Sato
Session Notes Taker: Tom Sato

Tags / links to resources / technology discussed, related to this session:

https://openid.net/wg/sse/

https://sharedsignals.guide/

Seeing SSI in Historical Context - exploring Europe first - then Asia.

Session Convener: Kaliya Young
Session Notes Taker:

Tags / links to resources / technology discussed, related to this session:

Link to a paper given by Kaliya at identiverse to set the scene for the discussion:
https://identitywoman.net/seeing-self-sovereign-identity-in-historical-context/

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

Kaliya started with a walk through the history of digital identity, from technical and then socio/historic perspectives, focusing in the introduction on the broader European historical experience.
See below for the presentation and and edited transcript.

Reason Taxation - Governments want to collect they want to collect money from you.
To Gihan's point, there is also an economic perspective from which to view identification. For example this is RMIT's paper on The Institutional Economics of Identity:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072823

Magna Carta 1066 - tracking for taxation person

Institutional Economics of Identity
Ability to tax.

Companies getting into it - is the last 20 years (yes digitally)
Church also wants to know who you are and collect money from you.

Paper gave good privacy from the holder to the Issuer.
Revocation is a problem.

Current IdP model - revocation is really great.

Decentralise ID world getting best of both worlds - has revocation and not be spied upon by the issuer.

Kaliya shared this link to
Becoming Artefacts: Mediaeval Seals,s, Passports and Future of Digital Identity

Kaliya mentioned the work she has been doing with people associated with radical exchange related to Social Identity.

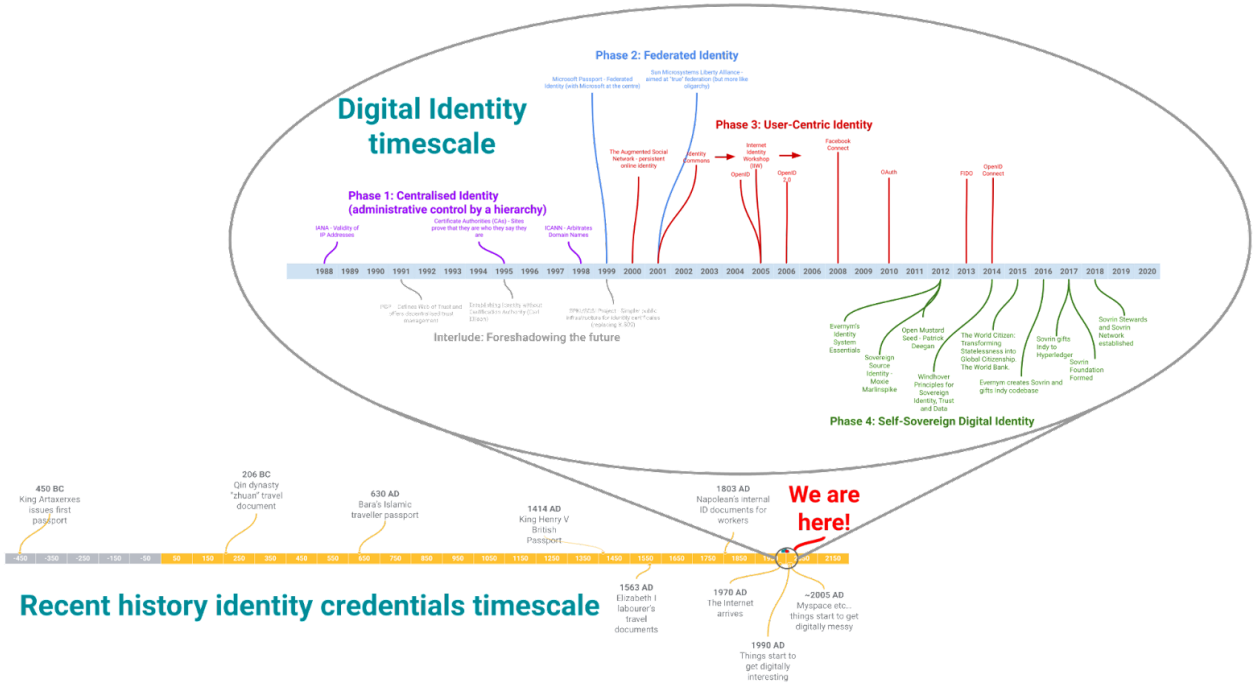
Kaliya pointed to Philip Sheldrake's critique of SSI

Heard about Japanese Ration Card - subsidise food to citizens. Distribute food fairly was motivation
Happening in Corona Age - japanese government - failure to provide fast subsidy to citizens because of lack of digital ID system - considering implementing to give out

Asia is a big place - not work to generalize - North America
Within Asia - there are many many things. I have no idea what happened during the time of the Kings before 19th century - British when occupied Sri Lanka - set up survey department - survey all the land they wanted to steal the land - before you steal it you have to know what you are stealing - you need to see if there are registered owners - So I think that history of colonialism - and set up in our country.

What happened with countries who didn't really get colonised.
60,000 years - of Australia - recent development take up a very tiny space of time of the First Nations people of Australia.

John P was referring to this image (and its extension, not shown, to a 60,000 year timescale):



https://www.goodreads.com/book/show/26740420-the-chinese-family-system

Japan has a family Tree system.
Mostly Men's names are listed - women's name are listed as "daughter or wife" but may not even have a name in that book.

Kin-Based Institutions - still has this feeling.
Running a company as a group - has a "family" feeling - work as a group

Kaliya made comment about being in western system that feels very alone.

I suggested it is not good or bad

Kaliya shared that

What is the purpose of an identity system?

Cultural belonging

History of ID in Thailand - short history of implementing ID system.
ID card only around for 100 or so years.

Then in fact we Thai people didn't even have surnames until 100 or so years ago - only began with "Proper" identification system began.

At first identity wasn't about "who you are" - it is about identifying which locality you belong - at the time what is considered first ID system. Document for someone who would go to a different locality in order to trade - someone who is governing the place where you come from - when going to the other place - you are not some no-body that no-body could trust - it was a trust document that would help you get to another locality - to know you are a trustworthy person to trade with. The king started not long after that Surnames emerged - then proper identity cards - due to modernization attempt at the time.

At that time Slavery was abolished - started to become one.

Gihan - would like to mention. Not traditional Sri lanka - what happened in colonial time - people when they get married - name, spouse name - name of father and mother - in marriage certificate - then you have to sign.

keep track of "who is who" those were on paper and not easy to search.
These two weaknesses in legal system.

Sign some kind of commercial document - my signature should be witnessed by two people.
This is not formalized in SSI type things.

When we build digital ID we should look at systems that were there before that - that we are duplicating that.

Witnesses - signing your signatures.

Taken over by "signature authority"

John Court - that is an interesting Question our DI stuff is focused on "authorities" to be more about reputational credentials coming from other people rather then authority that is centralized.

Imagine if something like facebook - couldn't post unless credentials from others that say you are mostly truthful -

Or you have a gold badge you are "truthful"

Populast people with profoundly un-true views.
I don't think things like reputational systems are reputational silver bullets.
Gihan.

Logan - i want to echo what John is saying.
Danger

Share things too easily.

Maybe we will ask for too much asking for information.

Other docs shared

There is also an economic perspective from which to view identification. For example this is RMIT's paper on The Institutional Economics of Identity:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072823

Edited transcript:

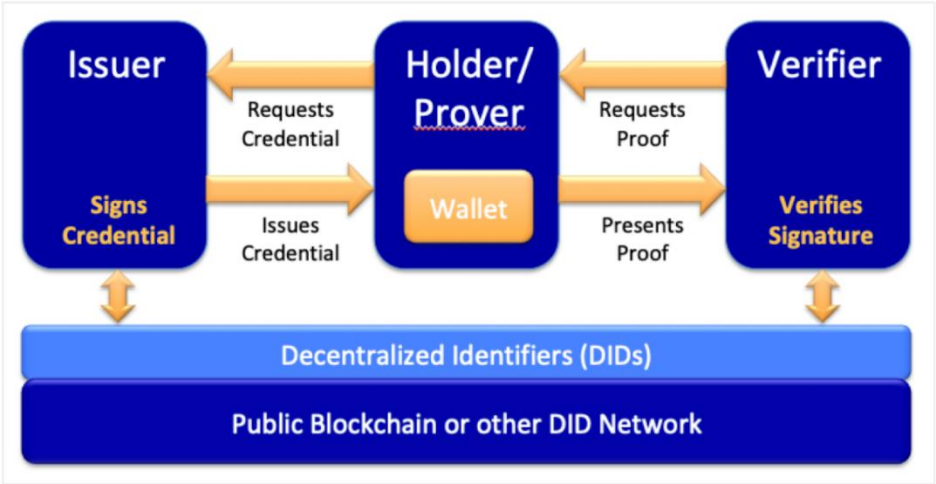
I published a paper on my blog and I also gave a speech at identiverse conference that I was going to go through the slides that I presented at that conference, just to share the historical context that I just, I, I have found and found really interestingthat is relative to the European context.

And then I'm happy to host a conversation about the Asian context which I know a little bit by No, I do not know enough to, to be a primary discussant in that but I am a skilled facilitator and then hopefully we'll have some key insights and sharing that can come from that.

So, um, this is the outline, so there's a materialist approach to SSI, an overview of SSI, a timeline of digital identity systems, which I'll go through very fast, and then we'll spend about

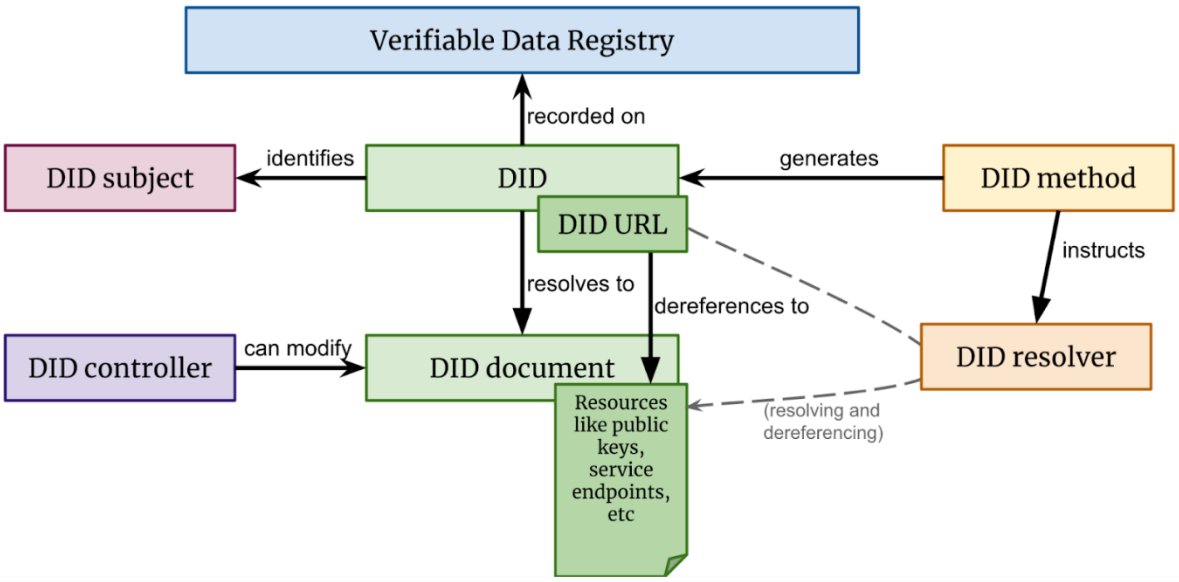
10 minutes talking about a timeline of identity paper based identity systems that arose in Europe, and then some contrast them and then this was an argument that I was making in the paper and it's not necessarily what the historical antecedents are in Asia and whether they line up with SSI or not and that's a great question. I love to explore in the second half and I'm not suggesting that they do. I just don't know enough, and I think we need to explore it further.

So, what the way that I understand the world is that everything is a process and it emerges in process of our time so that our lives as human beings and bodies are the result of processes, and that the artefacts that we create or point to and identify people and even things like identity documents are the result of processes you go through different steps to get the cards.



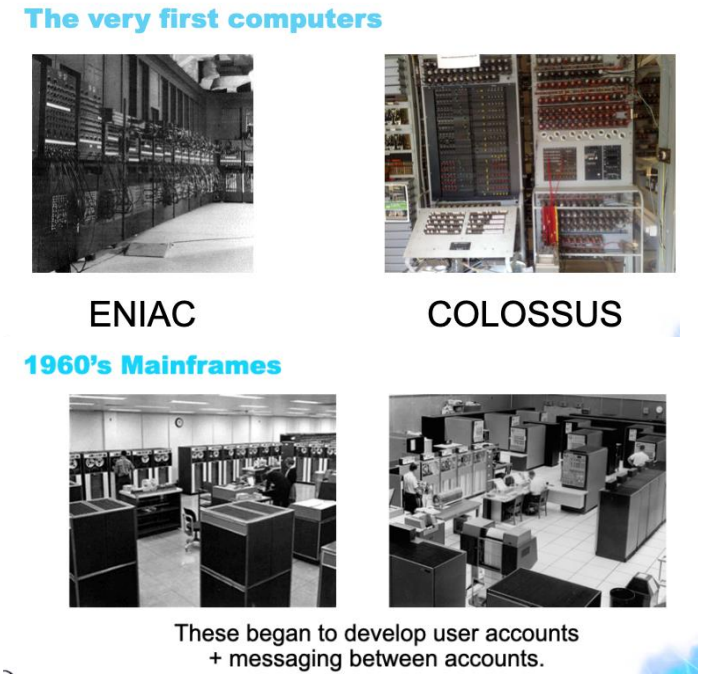
So understanding the process is really important when looking at identity because oftentimes, like “the thing” this is often over emphasised in identity systems like “the card”, “the credential”, but like how did those things come to be.

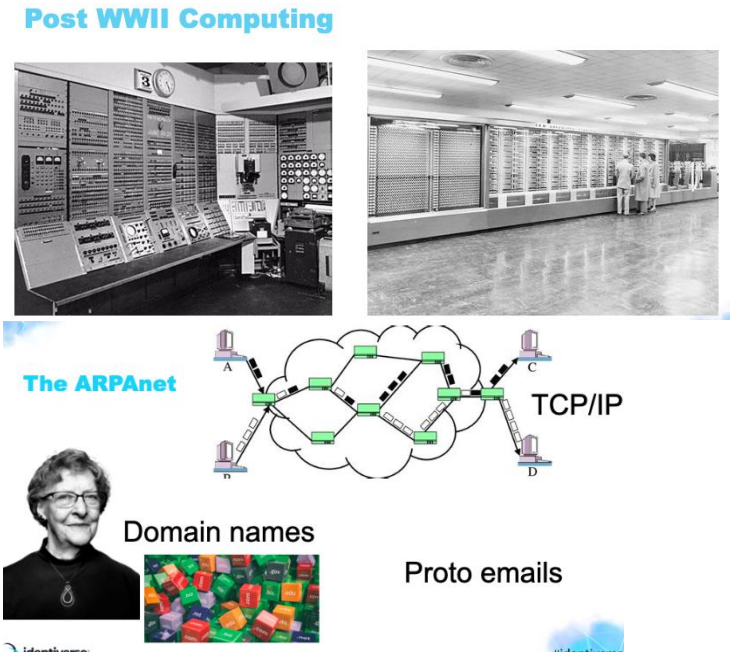
So this is the core SSI models that I'm sure many of you are familiar with, I'm not going to go into it. And then we have like DID explainer diagram.



I'm also not going to get into this either. But, oh this is not the right version of the slide show this is what happens in open space you propose a session.

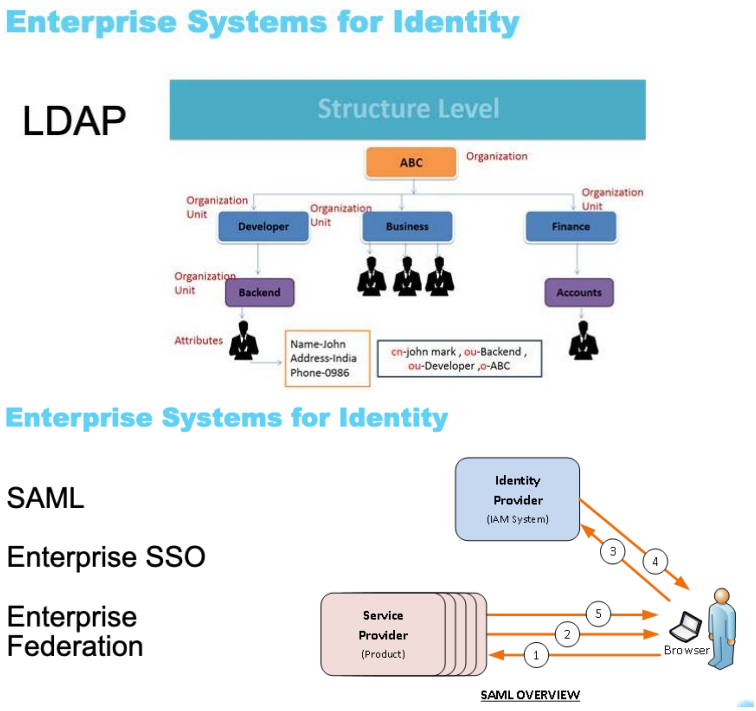
Okay. So as I explained timeline of digital identity system so the very first computers the ENIAC and the US and the Colossus in the UK, had no username and passwords because they didn't need to because they just did one thing, and it was operators that ran them but they didn't have accounts and starting after World War Two, these giant room size computers began to be built and university started using them.





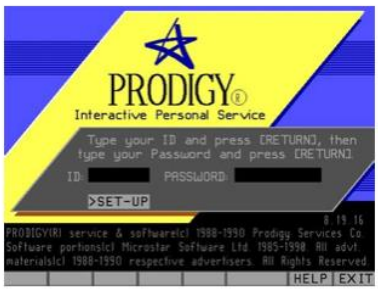
And they began to have username accounts accounts for different people using the computer at different times. These systems were linked together, beginning with the ARPANET and domain names were invented this woman, Jake Fleanor actually showed up at one of our internet identity workshops early on and shared her story, working in the lab where they first created the Domain name system.

Then we had the emergence of enterprise identity and access management systems that created l dap to sort of support different business units within a business being able to manage their own directories and share.



And then you had SAML enterprise self sovereign and enterprise Single Sign On an enterprise Federation's came out of this protocol stack.

Consumer Internet Beginnings

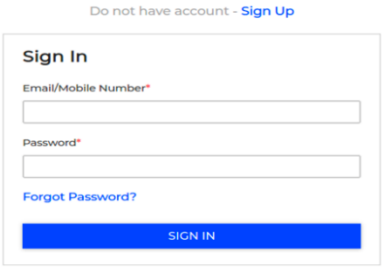


User-Name and Password

And you had the beginning of the username and password paradigm was transferred over to the consumer internet, in the early 90s. And it bled over into web one which was mostly content you consume with a little bit of e commerce happening.

Web1

- Mostly just content you consume
- e-Commerce -

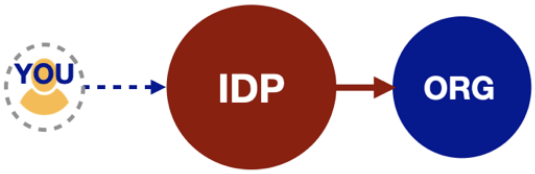


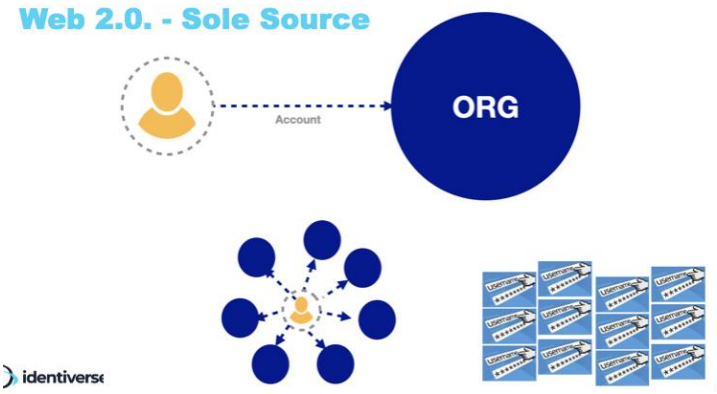
identiverse

And then with web with web two you had you had an ex, more and more accounts that you needed to create so somebody is not muted if they can mute that would be really helpful.

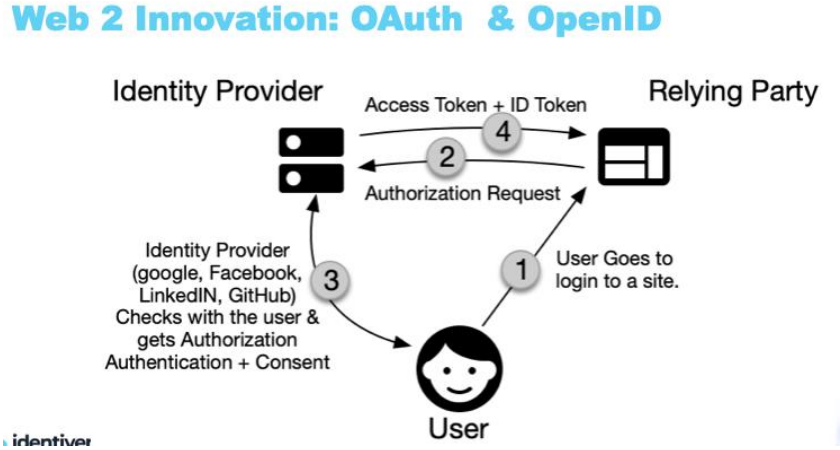
Web 2 Innovation: OAuth & OpenID

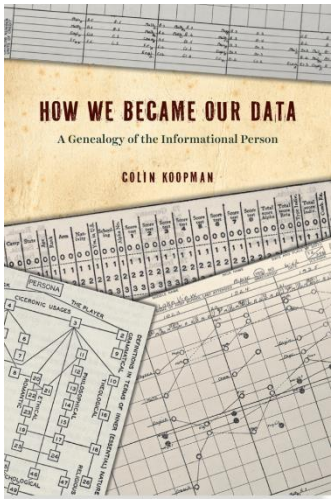
Identity Provider Model





And then you had open ID and o OS which are both innovated at the Internet identity workshop to reduce this kind of problem of so many accounts but it took the enterprise identity and access management paradigm and brought it into the consumer web and sort of ended up creating this identity provider model that we're still trying to address with SSI puts these very large companies in between you and the organisations you are connecting to. And so this is where we are kind of on today's web is this is the state of the art of where we were like five years ago. So that's sort of the web as we have it and now I want to share this deep context of why paper based identity systems arose and it should be qualified in Europe.

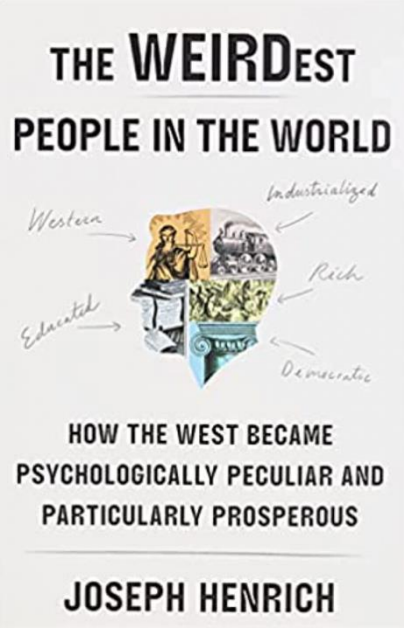




Because that's the context that I'm touching on. So during the pandemic I read this book called How We Became Our Data, a genealogy of the informational Person person, and it looks at sort of the the practices between 1900 and 1950 of bureaucratic systems documenting people.

And this is from the author a quote from the book,
I suggest that bringing the politics of information into view requires extending the scope of our historical analysis to the period preceding wartime information sciences and the postwar information theory to which they gave rise.

So he as a scholar of Information Studies kind of asked this question is like information theory was postulated in the very late 1940s and early 1950s and got widespread adoption very quickly and the question is why and it's because of the information practises that proceeding it so that that theory made sense.



And I also read this book during the pandemic. The weirdest people in the world. How the West became psychologically peculiar, and particularly prosperous. WEIRD is an acronym that says stands for Western Educated Industrialised Rich and Democratic.

So, the West is really weird psychologically compared to many other cultures on earth and the question is, why like how did that happen?

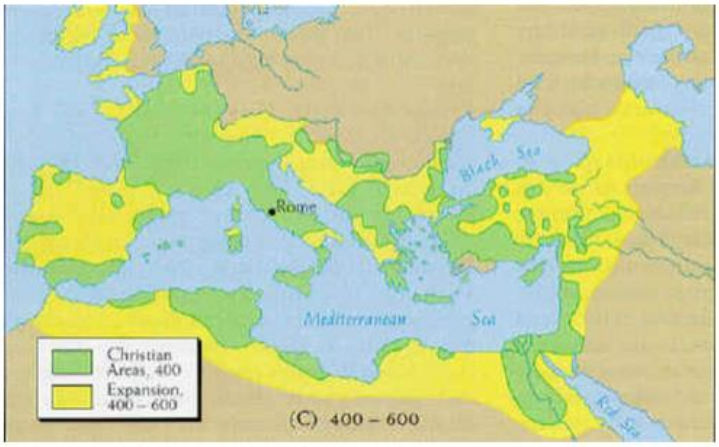
And many histories of modern identity systems beginning the Middle Ages with letters of introductions and first certificates and census receipts and citizenship papers that all were happening in various European countries. And it all, most of those sort of began around 1500 in Europe. But what happened before that that made this new practice of using these I paper based documents, make sense to people.

And that's what I put this dot together from the weirdest people in the world in our work, and in digital identity and thinking about this deeper historical context so why did this technologies, make sense to people, and what happened to make this technology

Marriage and Family Program

500 CE

Catholic Church Banned Cousin Marriages



And this map gives you the green is the area of Christians spread - up until 400, and the yellow is between then and 600 so hundred so 500 years ago with somewhere in between those two is the area that Christianity and specifically the Catholic churches had spread.

And so, they banned in this marriage and family program they banned cousin marriages, eventually, up until seventh cousins which is seven generations back or 140 years before you were born, he couldn't marry your cousins, that is far back. And they also banned marriages to people that you were related to but not by blood and this is where the term brother in law and sister in law comes from is that you were brothers considered brothers in law, therefore unable to marry them. So, if you were married to someone and they knew they had a brother, but the person you were married to died, you couldn't marry their brother, even though you aren't blood related to them.

So they really broke up, cousin marriages and this broke apart intensive kin based institutions that link people together based on family ties. And at the time, can be institutions did everything they organised production they provided security and they gave people a sense of meaning and identity, but you could never leave them because you were born into them, you might marry into a new king institution but even then back to cousin marriages people were keeping the power together in their kin networks. So, this is a sense of how far that Catholic Church and spread by 1000.

And without kin based institutions, individuals were both socially compelled and personally motivated to relocate seek out like minded others from bonds.

Monastery

Universities

Towns

They formed voluntary associations and engage with strangers. So, starting in the 11th and 12th centuries you have accelerated number of people moving to monasteries, universities, the first ones were formed and many many started forming in that time and towns formed where people migrated from the countryside away from their family and lived with strangers and at people that they would marry.

So this these new institutions and this breakup of family in kin based institution led to this proto weird psychology, which involves analytic thinking.

1. Analytic thinking: This grew in importance as people navigated the world of "individuals" rather than dense familial interconnections, reducing the importance and value of holistic thinking.

2. Internal attribution: As social life shifted to the individual, "traits like dispositions, preferences, and personalities as well as mental states like beliefs and intentions became important. Soon lawyers and theologians even began to imagine that people had 'rights.'"

3. Independence and nonconformity: "In a society with weak kin ties and impersonal markets," individuals focused on their uniqueness rather than venerating ancient wisdom and elders.

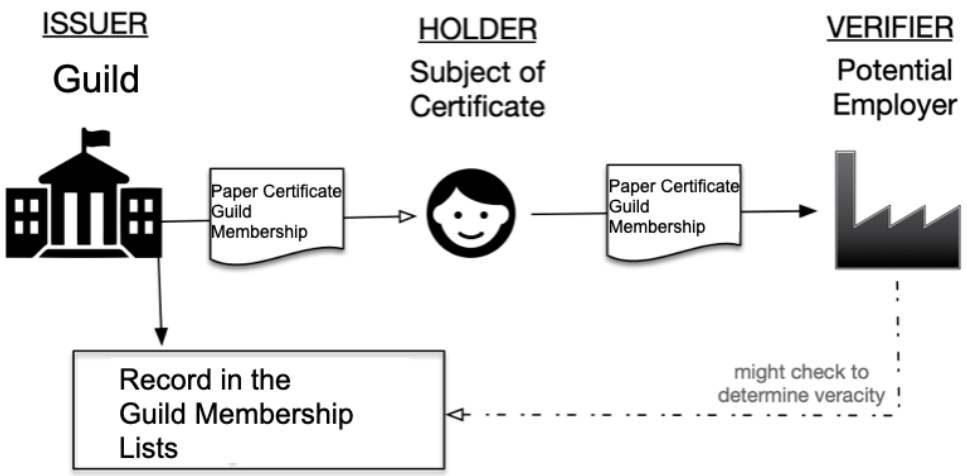
4. Impersonal prosociality: With life being governed by impersonal norms for dealing with strangers, "people came to prefer impartial laws that applied to their groups or communities (their cities, guilds, monasteries, etc.) independent of older social relationships, tribal identity, or social class."

"As intensive kin-based institutions dissolved, medieval Europeans became increasingly free to move, both relationally and residentially.
Released to choose their own associates—their friends, spouses, business partners, and even patrons… Constructing their own relational networks opened a door to the development and spread of voluntary associations, including new religious organizations as well as novel institutions such as charter towns, professional guilds, and universities."

But these new institutions needed tools to remember of who was part of an institution and who had left. And so I believe that the origins of contemporary institutions in the West and origins of identity documents are co intermingled so that guilds needed to know who their members are towns needed to know who their residents were militaries needed to know who made up, who were the soldiers and military uses units and hospital needed to know who their medical patients were.

And so, why did identity systems of of institutions emerge when they did and why did people choose to adopt these because these newly emergence assemblage were not defined by familial and genetic ties and people needed to find ways to support figuring out who has entered the boundary of the institution and paper based record keeping systems were available to do this it was a technology that could be leverage so there was a lot book of lists of people who had joined or were a part of an institution and they're also were cabinet files and index cards is another way.

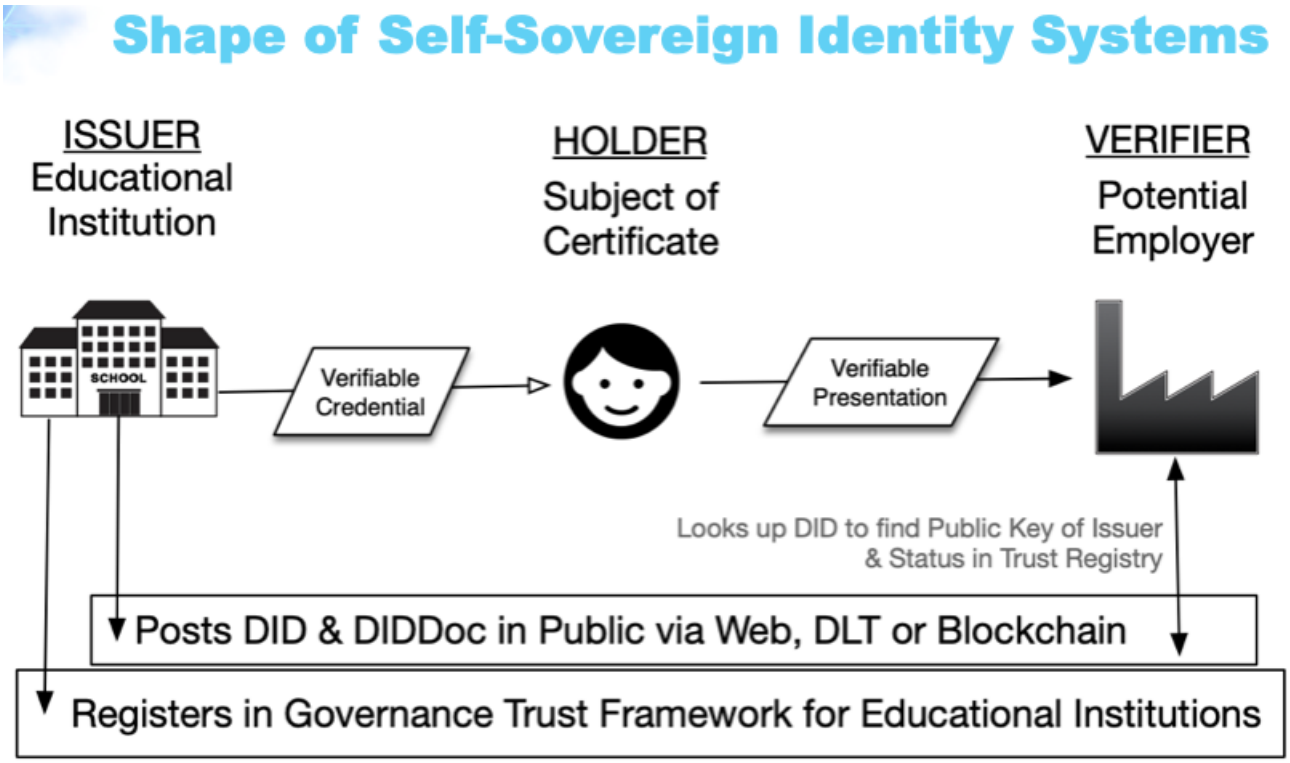
And these provided ways of keeping track of who was in a social formation or assemblage, and it could also involve letters of certificate given two persons given to the person themselves or letters of introduction that's sort of where these come from



So, if we look at a paper based identity system structure. you have a guild issuing a paper certificate to the holder the individual who is a part of the Guild, and the guild can present that certificate to a potential employer. And there's a record of the guild membership list kept at their headquarters and maybe the employers can I go check that right. And if we look at.

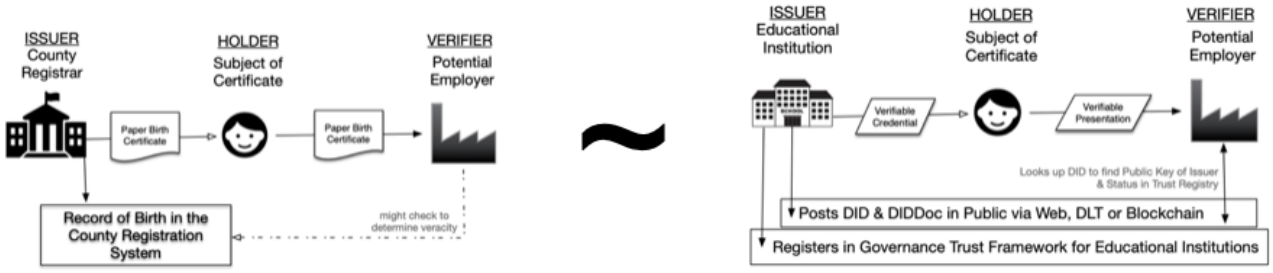
So if we look at this sort of where we left off and computer identity systems, this is where we left off with this kind of phone home architecture or back to the identity provider, which doesn't look like this, it looks really different and looks much more.

This is what a did arc, the SSI architecture looks like right like an issuer subject holder.



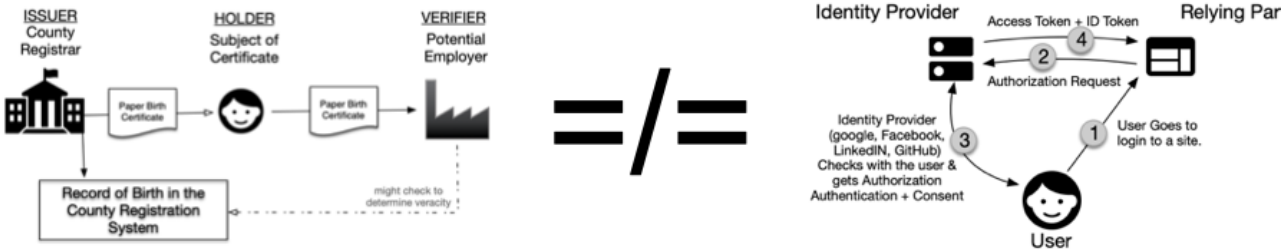
an alignment with the previous historical norms of how Europeans have been managing and constructing identity relative to people's belonging and institutions for, you know, 1000 to 500 years and those antecedents for why that makes sense go all the way

Alignment between WEIRD originated Paper Based Systems and SSI

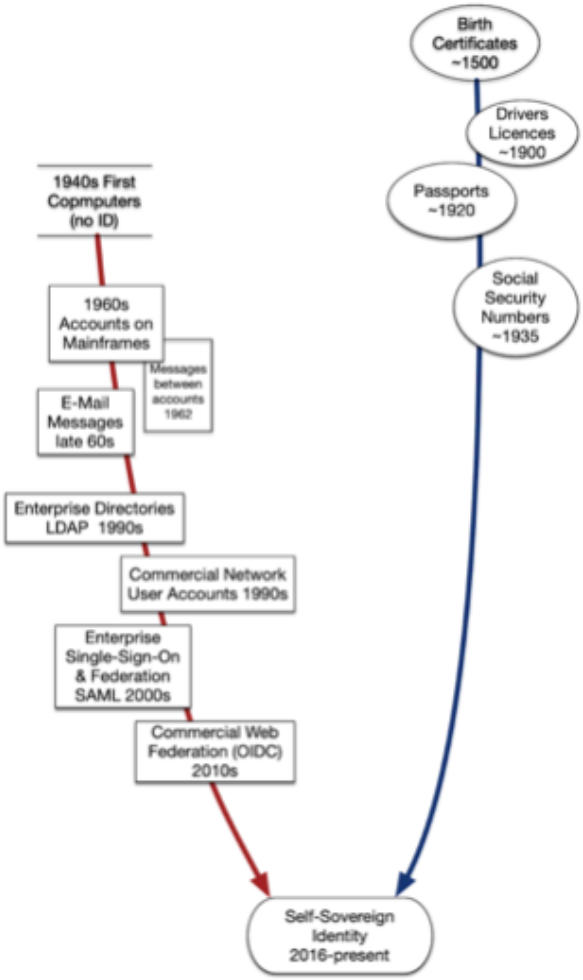


So I making the argument that self sovereign identity systems have back to 500 when the Catholic Church, with it's marriage and family practices started dismantling can based institutions. And that this shape of the paper based architectures that were prevalent in European context and cultures that have left Europe and gone to other places like America and Australia.

Non-Alignment between "Phone Home" Digital ID Architectures and WEIRD originated Paper Based Systems



They don't match this digital identity system which is partly why there's been so much pushback from Western liberal democracies to centralizing identity systems that require opinion the identity provider.



And then this is like a kind of putting these two things together that my argument in this paper is that there's a bridge between the digital ways that identity has happened in the past and this historical antecedents of paper based identity and that's self sovereign identity systems kind of bridge this gap and align with this historical way that emerged from managing identity on paper. So that is my presentation.

Session 2

Linked-Data based Verifiable Credentials with Selective Disclosure, Unlinkability, and Range Proofs

Session Convener: Dan Yamamoto
Session Notes Taker: Kazue Sako

Tags / links to resources / technology discussed, related to this session:

ZKP-LD Playground
https://zkp-ld.org

Paper: Appeared at Security Standardization Research Conference 2022 (SSR 2022)
https://sako-lab.jp/download.php?article=ssr2022_proceedings_dan.pdf

Slides
https://speakerdeck.com/yamdan/linked-data-based-verifiable-credentials-with-selective-disclosure-unlinkability-and-range-proofs

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

How do you include selective disclosure and VP to VC's issued by Japanese government?
-> we use special digital signature scheme called BBS+ for this purpose.

Standardization efforts for this type of VC have started in IETF and DIF.

Is there any revocation support?
-> Currently it is our future work.

How you managed range proof?
-> We used Bulletproofs to prove that the signed integer is in the range. This is a predicate proof.

Predicate proofs were known to be possible, and this is a working version.
The processing time is practical, but currently the size of proof is very large for this predicate proof.

The predicate proof is only for integers, not for decimal/floating number

Integrated Personal Data Store (iPWS) for Identity Wallets

Session Convener: James Schoening
Session Notes Taker:

Tags / links to resources / technology discussed, related to this session:

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

'Integrated' means a common data model for the individual, in the form of a standard ontology, namely, the MyData Ontology. See its Github at CommonCoreOntology/my-data-ontology: Provides a standardized extensible semantics for representing information about a person's profile. (github.com)

Mark Scott had wanted to attend, per his interest in "Digital Life Hub for use by anyone--envisioning a capability for secure storage and management of all things in one's digital life, implemented in a way that is worthy of trust and respects User Sovereignty."

For more information on this Linux Foundation project at IAM Project (github.com) To participate in a pilot, contact james.schoening@ieee.org.

Building a Privacy Community in India

Session Convener: Zainab Bawa
Session Notes Taker: Zainab Bawa

Tags / links to resources / technology discussed, related to this session:

https://hasgeek.com/PrivacyMode
https://github.com/hasgeek/topicmaps/ -
https://github.com/hasgeek/topicmaps/blob/main/Health_Records_and_Data_Privacy.png and
https://github.com/hasgeek/topicmaps/blob/main/Health_Records_and_Data_Privacy.png
https://sovrin.org/principles-of-ssi/

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

Typing notes from the end of the discussion to the beginning:

1. Cultural aspects of privacy need to be brought into consideration - especially lived experiences - before we speak about large concepts such as SSI and others.
2. The lack of alternatives to not complying to regulations is a disempowering experience, especially for individuals. How do we bring this issue to the forefront and centre of privacy debates?
3. Non-compliance to demand for biometrics or succumbing to facial recognition requirements, especially in the case of children is tricky, again owing to lack of alternatives. One of us shared the experience of our children's data being asked for by schools and parent(s) trying to educate the school authorities about privacy and data protection. This point led to the discussion about the cultural contexts for privacy and what privacy means in essence to each one of us.
4. We discussed the lack of awareness about the costs to privacy and how to help the earlier generations and generations before us to evaluate. We shared examples of how to evaluate the trade-off between buy adware phones which cost INR 5,000 less than a phone that is not adware, and to recognize that spending INR 5,000 extra is a lesser trade-off than foregoing individual privacy.
5. There was a brief mention about how compliance to identity systems (and perhaps their conceptualization) is embedded in a patriarchal mindset - of a patriarch (technology/institution) holding your data in a benign manner.
6. A concern was also raised about how countries like India demand biometrics and other forms of the individual's identity for immigration, making appointments with doctors, etc without any information to the citizen about where this data is stored, who will access it, and who will process/use this data in future.
7. A question taken from an earlier session on "what SSI means for Asia" was how to deal with the institutional complex which demands adherence and compliance versus the need for personal data privacy and SSI.
8. There were some discussions around India's data protection bill and the inclusion of non personal data in the bill. Adding links here to Privacy Mode's NPD study -

https://has.gy/bFon Also adding the critique of the agriculture data management policy which ignores that non personal data flows from personal data - https://has.gy/naQc

9. Building a privacy community in India has involved doing the following:
    1. Defining problem statements.
    2. Creating activity maps with broadly defined outcomes.
    3. Aggregating experts around forward topics, and around immediate topics/issues. Creating knowledge outcomes, including practice guides and playbooks on doing data governance, governing health data, etc. For example - https://hasgeek.com/PrivacyMode/bpg/sub Get organizations to share their knowledge and journeyman case studies in order to exchange ideas more freely, and for adoption of good ideas and practices.
    4. Focus on technology, data governance and emerging tech-policy issues as three buckets to work with for the privacy community.
    5. Bring practitioners into conversations with policymakers for the spread of ideas. For example - https://hasgeek.com/rootconf/navigating-cert-in-directives/sub
    6. Continue the push for new sets of practitioners to interact with governments and policies at various levels.
    7. Build a group of practitioners/experts who can be available for steering the community. Rotate stewardship.
10. We briefly discussed the following points about community building about privacy:
    1. Defining problems/problem statements that can bring focussed groups of people together.
    2. Building forward-looking activity maps from the problem statements.
    3. Building the community in a modular fashion. See Architecture of Participation - https://weareopen.coop/aop/
    4. Continuity of communities - via monthly meetings and meetups.
    5. Tools for community building - keep these simple, and allow for maximum participation at minimal time, attention and human resource costs.

NEXT STEPS?
Will you take any Next Steps and/or continue this conversation? YES!

Build communities of concern and influence

If so, can others from the workshop join? Yes

If YES please provide Contact Information for those who are interested:

Zainab Bawa - <PrivacyMode@hasgeek.in>
Munir Mohammed <m.mohammed@ieee.org>

Is SSI-on-Blockchain is Objectively a Bad Thing

Session Convener: Sammotic Switchyarn
Session Notes Taker: Catherine Nabbala

Tags / links to resources / technology discussed, related to this session:

https://weh.wtf/ssi.html

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

- Proposed alternatives to blockchain: KERI
- Are Enterprises concerned about using "blockchain" or having their problems solved?

Links shared:
Self Sovereign Identity ≠ Blockchain - Jolocom
https://jolocom.io/blog/dezentrale-identitaten-not-blockchain-2/

2. SSI-on-Blockchain is Objectively a Bad Thing | Niko's Blog (weh.wtf)
https://weh.wtf/ssi.html?utm_source=substack&utm_medium=email

3. Do You Need Blockchain for Enabling SSI? | by Affinidi Pte. Ltd. | Affinidi
https://academy.affinidi.com/do-you-need-blockchain-for-enabling-ssi-452d62b3489

All You Wanted to Discuss about Aadhaar

Session Convener: Sankarshan
Session Notes Taker:

Tags / links to resources / technology discussed, related to this session:

https://uidai.gov.in/
https://www.mosip.io/
In Pursuit of Proof - A History of Identification Documents in India - Tarangini Sriraman (link)
Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present - Keith Breckenridge (link)
Berg, Alastair and Berg, Chris and Davidson, Sinclair and Potts, Jason, The Institutional Economics of Identity (May 25, 2018). Available at SSRN: https://ssrn.com/abstract=3072823 or http://dx.doi.org/10.2139/ssrn.3072823
Prints in the sand of time - The construction of uniqueness before biometric authentication
Critique of Aadhaar - Rethink Aadhaar page

Paving a Digital Road to Hell: https://chrgj.org/wp-content/uploads/2022/06/Report_Paving-a-Digital-Road-to-Hell.pdf

Key Differences Between the U.S. Social Security System and India's Aadhaar System
https://www.newamerica.org/fellows/reports/anthology-working-papers-new-americas-us-india-fellows/key-differences-between-the-us-social-security-system-and-indias-aadhaar-system-kaliya-young/

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

1. How communities are built via a modular approach?
2. Involvement and participation.
3. Building knowledge and community of experts.

2008 there was a particularly violent terrorist attack - fall out of that attack was that the state and central government - we have a number of identity documents
They has passports
electoral photo ID cards
Other cards -
NO way to uniquely identify people.

Unique number - for each person with certain criteria.
Aadhaar (at this point in time) is not "a card" but just a number.
Access services via consolidated number of India

Because this is a gigantic initiative - and needed to be sold on.

Not exactly true - had to furnish two pieces of existing documentation - who you were and where you live - then you were issued Aadhaar number - two reasonably valuable credential get a third one.
Not supposed to be publicly shared - on different laminated cards.

“Voluntarily mandated”

Aadhaar begins to be a key (essential, mandatory) link in getting access to services.

The voter id card, EPIC, is supposed to be linked to Aadhaar to allow de-duplication. This causes complex legal overlaps between separate government bodies, and interests.

Goal to clean “voter roll”
Election commission has own stuff.

Biometrics now - this is different.
Fundamentally transactions linked to - “gold standard identifier” use eKYC and KYC also linked to Aadhaar

Three questions:

1. is Aadhaar fool proof - can you create fake aadhaar - depending on definition - you can.
    1. Hanuman has one
    2. Aadhaar biometrics forged easily - now check for liveliness based on certain checks.
2. Does Aadhaar create exclusion - documented no matching - no way to fix biometrics unless you have extensive access
3. What happens to Aadhaar if you are no longer a living person - because you can’t lift biometrics of dead body - linked to mobile phone. new they will introduce Zeroing out number. Next of kin have to continue pay subscription charges - will give number will go over to new number - cyclical problem is created. Because number of folks didn’t consider entire point.

Applicable to Infant - had an Aadhaar entry created - so they could be admitted - 5-6 months - collected biometrics - but they are useless

Had to go property tax - brought aadhaar card
extensively used in Banking
only thing happened - scope of things that can be used for Aadhaar KYC - reduced scope via supreme court - reduced number of scams.

General Attitude
Aadhaar is a good thing. (anything that removes friction from interactions with Government is a good thing)
UPI - (Payments) it is seen as a good thing., being propsed as what north americans should be looking at.

Talked to folks who have
problem dealing with “faceless entity” raise ticket - make a call to do that. No ability to walk to a person. Digitization - is growing - talking to a system not a human. Talking to a system is difficult if you don’t understand it.

Employs poverty fund.
Your EPA
4-5 months to get linking sorted -
they were not doing look up properly.

PAN - permanent account number
supposed to be linked - name on Aadhaar didn’t match - linking failed.
update income tax return name - to Aadhaar name

When works - works nicely enough - but when it doesn’t it can make you feel upset.

What is next for Aadhaar?
I think the significant number of evolutionary changes.
Get “link proofs” in our speak.
Core COVID vaccination - linked to Aadhaar - and then passport - none of it actually worked.

Aadhaar is also foundational for National Digital Health Mission.
Basis stipends and scholarships.

Identity framework - serves a bunch of integrated activity - enourmous investment from governmetn building off aadhaar.

Aadhaar is going to be used to meet original goal - can we have a central registry of “all indian” unless you actually take an indian citizenship - it is only at tha tpoint in time you get a citizenship. As naturalized citizen - no paper that says I am citizen - on passport….

Aadhaar is continuing to be used to populate national population register.

Add more systems in - one number to rule them all.
one number to which a whole bunch of things are linked.

Kaliya shared slides from her research trip to India.
https://www.slideshare.net/Kaliya/aadhaar-identity-north-presentation

more and more systems
who is auditing them to make sure they meet strigient standards.
They don’t have paths / road maps.

Trustless wallets - doesn’t matter where you put your information - is it verifiable - is it changed or the rest of it - shouldn’t matter where you hold it.

Does it match the presentation model to be able to present on own behalf. Would have to re-factor whole supply chain.

See Technological thought process going into Aadhaar 2.0
The inherent risks of relying on technology that is inherently untrustworthy (source code quality/review production etc. Wallets based on code that isn't audited or controlled).

who is going to promote this - a government thing.

MOSIP is a digital public good
including
Project framework for everyone outside of india that wants to take a Aahaar like approach - unlikely to be system that will power aadhaar in the future.

is SSI aware.
challenge with MOSIP for business
default to design patterns that are not modern
very biometric heavy

seen MOSIP - it is the preferred solution for the biometric national foundational ID - governments now believe they need to have a database of everyone's biometrics - not a complete solution. It is the one that the government that feels like it needs to give veryone "platic cards" need to have a central biometrics registry - no evidence in any interest in doing otherwise

if it is going to be mosip it is something we can live with.

iprove is doing liveness checks.
we sezu and are weary of them.

centralized biometrics scare us - if they do them badly they are terrible.
doing architecture don't concentrate in one place

unles we have done
OCR labs

Eric - very good point - proovine self to device - apple/google/huaway intermediate - need to trust.

CRVS - de-duplication ability to equitably distribute services.

Biometrics and trust is a huge hurdle

Session 3

Strategies for Resisting Vendor Pressure on Governments Equating "digital-id = biometrics"

Session Convener: Eric Welton
Session Notes Taker: sankarshan

Tags / links to resources / technology discussed, related to this session:

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

Identity Week Asia is more crowded with biometric vendors who position that a digital ID is in a central repository set up by the government - this is at odds with what SSI folks discuss

Other vendors think about this in terms of proprietary credentials - non portable and of unknown standards. Digital ID is seen as “government property” much like a passport

There is huge spending and lobbying to pivot the thought in government circles to the above (which is kind of a MOSIP.io model - the open source framework which then gets integrated with proprietary biometrics)

Nobody needs an identity - but credentials which can prove things about them. “A digital identity does not exist”

Digital National ID - could be a credential. This can form the foundation on which other things can be stacked. “Singpass” as an example - has the ability to sign documents - National PKI? integrated with MSFT, Adobe etc Can be used for interactions with the government.

Biometrics vendors are interested in selling devices

Contactless fingerprints are high quality but struggling to get NIST recognition

electronic signatures (ESRA) - facing issues around notarial functions in at least seven US states

The commercial consideration of identity projects seem to influence more biometrics based designs

For national projects vendor lock-in allows for stability and fixed costs - often desirable.

There is opportunity to have the discussions with the correct contexts which can span sectors

In terms of strategy the focus on economics is one of the key aspects. And the technical one around federation

Lead conversations with solutions - use cases and exchange of value. Also demonstrate the potential of the business (and not being limited to devices)

Governments in SE Asia are attuned to optics. Social movements have a part to play in creating substantial influence around data, digital ID and biometrics

Identity = Biometrics = set of records in a government db : the common perception of ID - and this is propagated in conferences like ID4Africa and Identity Week - both of which are heavily focused on selling biometric systems to governments for national identification systems, although both, and specifically ID4Africa, have begun a shift to a broader understanding of digital identity.

In general, the biometrics-as-id crowd is wholly disconnected from credentials, and those that understand credentials as the future market are pushing vendor-lock in and proprietary formats. This works in formats where credentials are not yours, but are government property, much like a passport.

We did recognize that foundational credentials, such as those operated by a government, definitely play a role - specifically in enabling legally binding digital signatures, where legally binding implies recognition by the government which issues and supports the foundational, biometric id.

Side digression: contactless biometrics are in a battle for NIST and FBI acceptance which is blocked by biometrics device sellers who are threatened by biometric capture based on ubiquitous cameras. Not unlike the challenges to online notary in u.s. states which delegate that responsibility to lawyers who are protecting their revenue streams by requiring in-office visits.

returning to the discussion of strategies to combat the “digital id = biometrics” push introduced the idea, from several participants that the core concerns are economics - we must respond to economics with economics.

- rather than focus on data, or data-privacy, focus on the economics of data and the value of monitoring “proper use” and respect for digital rights as a way of preserving the economic integrity.
- an example was provided of a recent Vietnamese government official who suggested privatising district level personal data for corporate game, but who is now in jail for embezzlement

A salient point was made that if we propose change, we have to demonstrate value, we cannot simply propose change on the strength of technology. This requires a level of detail that focuses on verticals and ecosystems (value-chains) driven by credential production and exchange.

We briefly discussed the extent to which policy drives ecosystems or ecosystem adoption drives policy. In a nutshell - do not lead with ID, lead with ecosystem value chains and indicate that coherent policy requires coherent id.

Conversation shifted to the topic of optics in national id, and an example came from forestry in Cambodia - where a concession was granted to a harvest a national park and, as is typical in asian societies, the concession was granted between government and private sector elites. This resulted in a huge outroar on social media, which - because it created negative optics - resulted in revocation of the concession. This suggests that focusing on the negative optics of digital id = biometric id is a vehicle forward in asian societies.

Further discussion addressed the difference and difficulty in conveying digital id concerns to less digitally literate populations. For example, where destruction of a national park is easy to understand, subtle control or subversion of a public key infrastructure is akin to hidden magick.

One suggestion as to how to deal with situations where you are literally standing next to someone advocating total surveillance and a collapse of privacy is to reflect back on the advocate - pointing out how the surveillance and privacy violations would reflect on them.

The next suggestion was to point out the vast governmental cost of retaining surveillance and privacy-adverse central data, whereas local biometrics have a significant advantage. This advantage is in line with the technical concerned voiced earlier regarding the extreme risk of central profile storage.

Wrapping up the conversation was the recognition that, despite often being brutal and intrusive, the governments of southeast asia are widely perceived as protecting their citizens. Using the standard authoritarian play, drumming up fears within the population allows the government to position itself as the only path to safety - and if they need your biometric id to be your digital id, then so be it.

How Organizations Can Make and Save Money with Decentralised Trust Models.

Session Convener: John Phillips
Session Notes Taker: Jo Spencer / Thomas Robin

Tags / links to resources / technology discussed, related to this session:

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

Traditional v New Models of Value Exchange

Sezoo (www.sezoo.digital) is focused on advisory / consulting

Digital Trust $58b opportunity globally.

⅓ of employees in the US are working in "trust" (checking stuff)...

Are these right? Not likely…

Shipping market analogy - need to think about the digital economy that can be enabled - not the cargo process, the ships etc.

Issuer - Holder - Verifier models - underpinned by different technologies…

Centralised - Federated - Decentralised models and how actors tie in
6 transactions to consider in a decentralised model :
1 : Issuer - Holder
2 : Holder - Verifier
3 : Issuer - Governance Framework
4 : Governance Framework - Verifier
5 : Holder - Governance Framework
6 : Issuer - Verifier

When moving to decentralised models, a "Why should we?" is often a pain point.
Often due to liabilities in who has to take responsibility.
Third parties trying to solve trust issues (KYC, etc) is a false solution as they would only be relied on because the issue is complicated. If it becomes a simple or easily verifiable, contracting TP becomes irrelevant

How would new decentralised models meet specifics requirements ?
Using a 3 step process, it becomes possible to rank use cases, filtering and scoring them to finally obtain their ranking.
Example filtering :

Is it simple ? Is it under the right control ?
To score :
- Reach
-Benefit
-Perception
-Change Readiness
-Impact

Using a graph it is then possible to drive the discussion around the uses cases displayed

Recap of where the money will be :
- Ensuring data is authentic
- Providing services to verify data or issue verified data
- Interpreting the verifiable data from different sources

Wallets is a complex but fraught space

An expectation on decentralised models is that the numbers of Governance Frameworks will be lesser than Issuers who will be lesser then Verifiers trumped themselves by the number of Holders.

Product opportunity as a result will be in providing services to the last 3 and making it the most seamless into existing processes.

Future is to make things easier without needing to go into too much details

DIDComm for IoT Use Cases

Session Convener: Masayoshi Mitsui
Session Notes Taker: Kazue Sako

Tags / links to resources / technology discussed, related to this session:

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

Assumption & Motivation

- IoT has become the centre of the Internet (trillion scale)
- With the spread of IoT, more IoT devices will handle sensitive data like payment, vital, business document, energy, and privacy data
- Around 2010, computing resources and models moved to mobile-cloud, and in the next 10 years will move to edge-computing and IoT devices.
- Through this session, I hope that more people will become interested in IoT systems with DIDs, and that more people will create use cases to utilise DIDs to address real-world challenges that IoT systems face.

Market Challenges: difficult to solve with conventional digital ID technology to build trusted data distribution in IoT systems.

- Manual device provisioning with CA, PKI
- Device key management with root of trust (like linux/TMP, Arm Cortex TrustZone, Renesas SCE)
- limitations in building secure communication channels on a specific transport
    - Typically, an IoT system consists of multiple IoTs, servers and data centres. This means that data flows through multiple pathways and communication protocols, passing through brokers and message queue caches, crossing NATs/firewalls, and reaching its final destination.
    - Communication between IoT devices and the cloud is not assumed to be bi-directional and session-based communication
- Even top-tier makers lack security experts and budgets, so it is hard/impossible to build e2e secure channels between diversified endpoints for a wide variety of product lines.

Introduce "UNiD"

I take on the challenge of developing an open-source and scalable end-to-end secure messaging solution for IoT, named "UNiD" using features of decentralized identifiers (DIDs) as a basis of security and privacy, and it is built atop DIDComm messaging protocol which works over any transports, it makes end-to-end messaging reliable, secure, and easy.

Github: https://github.com/getunid/unid
Demo: https://www.youtube.com/watch?v=ha37sXN_Sec

We're developing it in collaboration with silicon makers and global makers.
Looking forward to collaborating with you too.

Discussion Topic

- Security & Privacy Considerations of DIDComm
- DIDComm is sometimes referred to as reinventing the wheel, but clearly an overlay security protocol is necessary for modern systems consisting of a wide variety of endpoints.

Are there any notable IoT use cases?
-> The issue in the IoT space is addressed in IETF as SCITT(Supply Chain Integrity, Transparency, and Trust), too. I don't sure about SCITT in detail, but they are also using DID/DID Document as issuer/signature verification.
https://datatracker.ietf.org/meeting/113/materials/slides-113-secdispatch-trustworthy-digital-supply-chain-transparency-services-00

For forward security, we can consider PFS on DIDcomm. Example use case?
-> You want to ensure the data authenticity through office equipment, like a scanner, who will forward the scanned data to the selected entity. Even if the secret key is leaked from the device, the confidentiality of previously encrypted electronic documents must be protected.

Is the forward secrecy solved in DIDcomm?
-> Discussed in section 5.1.5
https://identity.foundation/didcomm-messaging/spec/#perfect-forward-secrecy

How does DIDcomm help encrypt the data?
-> You can use Diffie-Hellman key exchange using DIDcomm. (The feature itself is included in DIDcomm.), ECDH-1PU
https://identity.foundation/didcomm-messaging/spec/

How does UNiD communicate between device and cloud?
-> In the prototype, send Enc(VC(m)) through DIDcomm on MQTT.

What if a malicious person builds a malicious IoT-hub?
-> With UNiD, you can set up an endpoint of a trusted entity as the initial profile for their devices.

Are there people working in using DIDcomm for IoT?
-> Yes, there are people at Sovrin working hard on this.
https://sovrin.org/library-iot/

Is DIDcomm reinventing the wheel?
-> It was originally for messaging. If you start communication, there might be some overlap.
-> IoT cases are often simplex and asynchronous communications due to their highly constrained nature, and there are many different transport combinations. It is very expensive to build a secure communication channel for each transport. When IoT data crosses multiple systems to reach its

final destination, a vulnerability in any of the communication channels will undermine the reliability of the system. There is value in being able to implement a transport-independent protocol for sending verifiable messages from a device to its final destination.

Which network layer in OSI layer does DIDcomm belong to?
-> Daniel Hardman@evernym had a good explanation on this.

Are there privacy enhancing features in DIDcomm?
-> It would be nice to combine DID with FIDO. Adding Zero-knowledge proof is another option.
Current features seem enough for current use cases.

How do you learn the DID of the device?
-> When it comes to UNiD, IoT device manufacturers can set up an endpoint of a trusted entity as the initial profile for their devices.

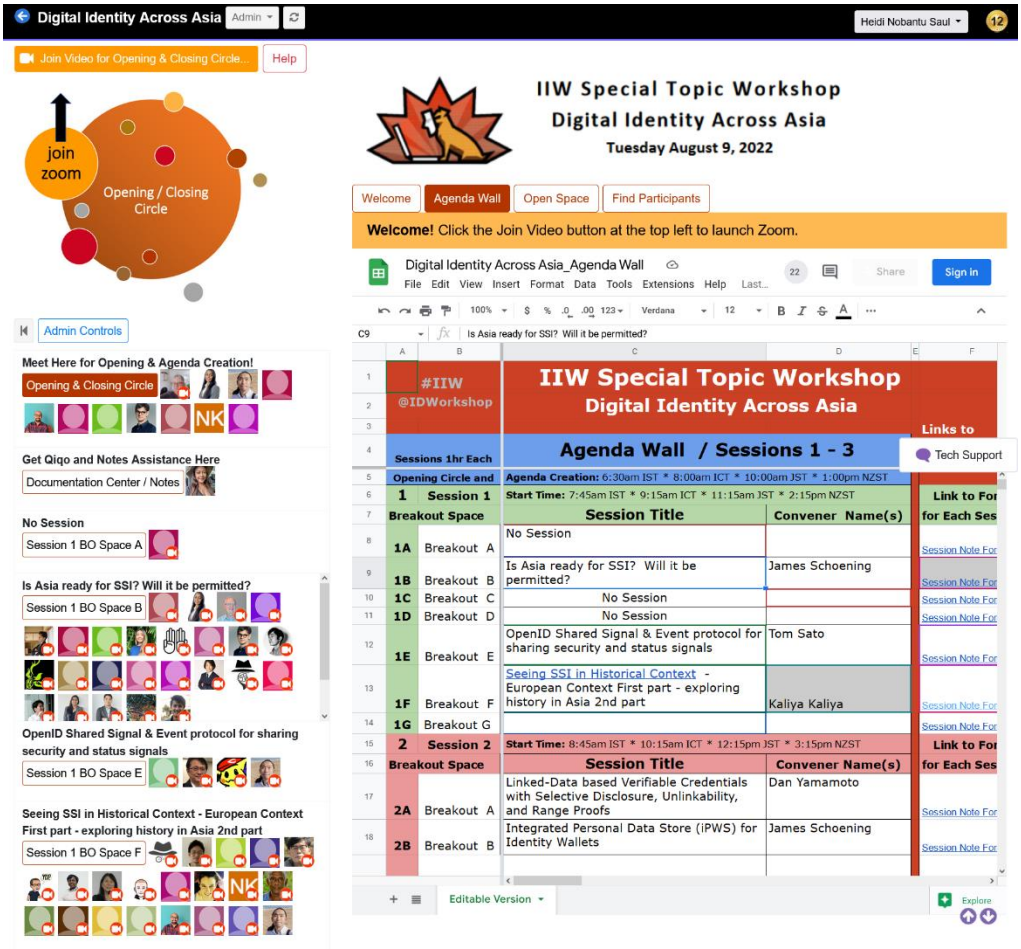
How do you know the genuineness of the device?
-> When it comes to UNiD, IoT device manufacturers can set up a secret param as the initial profile for their devices.

As a result of attending Digital Identity Across Asia

***** Please complete the sentence: As a result of attending Digital Identity Across Asia …. *******

- *… re-innited my interest in this area, and showed its potential*
- *…. i was inspired to see the growth in our regional community*
- *.. I was able to show that there are people in Japan trying to make DID/VCs real!*
- *Motivated to continue delivering this kind of solution. There is still hope.*
- *I didn't have to explain why identity is important to likeminded people :)*
- *several people from differing areas of discipline were able to share information that normally goes more unnoticed. This is of great benefit to the community as a whole.*
- *I've come to think about a lot of things that didn't cross my mind before.*
- *… I am convinced that Asia will emerge as next big consumer of the RIGHT solutions for Digital Identity leveraging DID/VC, etc.*
- *… I got to know about the work going on in digital identity and SSI space and adoption state of the technology.*
- *… am encouraged about the activity in this space in the region!*
- *I loved the innovation in the region - super exciting !*
- *I really was happy to discuss so many VC/DID/SSI things under the sun (daytime in Asia)!*
- *… I am getting a chance to get more update about the situation of SSI/VC/DID in Asia :)*

… have a good idea of the topics and issues to examine across the countries in this region.



Closing Circle ZOOM Chat

23:17:37 From Prustar to Everyone: This has been so great!

23:18:52 From Kazue Sako to Everyone: I enjoyed it very much! Thank you for those session organizers.

23:20:15 From sankarshan mukhopadhyay to Everyone: +100 for Ayanworks! Thank you!

23:20:27 From Eric Welton (Korsimoro) to Everyone: thank you

23:21:32 From Catherine Nabbala to Everyone: What a great start! Thanks to you all for making it happen!

23:27:49 From Kirankalyan Kulkarni to Everyone: This is a starting point and I am sue we will have more participation next time

23:28:21 From Gihan Dias to Everyone: 👍

23:30:25 From Zainab Bawa to Everyone: Have added notes for the privacy community discussion

Key pointers were:

1. Cultural challenges to privacy
2. Lack of alternatives to non-compliance

3. Awareness about privacy trade-offs with costs.

23:32:27 From Kaliya Identity Woman to Everyone: https://www.slideshare.net/Kaliya/aadhaar-identity-north-presentation

23:32:39 From Kaliya Identity Woman to Everyone:

https://www.newamerica.org/fellows/reports/anthology-working-papers-new-americas-us-india-fellows/key-differences-between-the-us-social-security-system-and-indias-aadhaar-system-kaliya-young/

23:32:48 From sankarshan mukhopadhyay to Everyone: The notes for the Aadhaar session are excellent - thank you, Kaliya!

23:39:26 From Sammotic Switchyarn to Everyone: https://weh.wtf/ssi.html

23:47:55 From Kirankalyan Kulkarni to Everyone: oh that's great to know..

23:48:08 From Eric Welton (Korsimoro) to Everyone: better printers?

23:48:56 From Masayoshi Mitsui to Everyone: Thank Paul for great comments & Sako-sensei for awesome taking note 🙂

23:49:29 From Paul Grehan to Everyone: Thanks Masayoshi & Dan for some awesome presentations !

23:49:44 From Masayoshi Mitsui to Everyone: I have the next meeting, so if you'll excuse me after you.

If anyone is interested in DIDComm/IoT Usecase, please reach out to me: mitsui@collabogate.com

23:50:16 From Dan Yamamoto to Everyone: Thank you Paul to mention our work 😄

23:51:20 From John Phillips - Sezoo to Everyone: Good recollection Eric! :)

23:52:19 From Heidi Nobantu Saul to Everyone:

23:56:34 From Jo Spencer - Sezoo to Everyone: +1 Eric!! Thanks for your input!

23:57:07 From John Phillips - Sezoo to Everyone: +1 for daytime Asia

23:57:29 From Kirankalyan Kulkarni to Everyone: Yeah +1 for day time

23:58:54 From Eric Welton (Korsimoro) to Everyone: @Catherine - Thank you for mentioning that. Once a month - Daytime in Asia - joint DIF/ToIP call much like this.

23:59:28 From Prustar to Everyone: Thanks everyone for a great session - I have to sign out now 👏🏽

23:59:34 From GeunHyung to Everyone: i am very happy to get a SSI meeting in Asia region.

00:00:12 From Eric Welton (Korsimoro) to Everyone: gotta run to next meeting - thank you everyone!

00:00:53 From sankarshan mukhopadhyay to Everyone: thank you so much. Look forward to seeing all of you again soon!

00:00:59 From Catherine Nabbala to Everyone: should you be interested to join our monthly calls. Thank you https://docs.google.com/forms/d/e/1FAIpQLSdFgi15NWrXL_-HM9KkL1IQ0uTBZAUgLN-03lvFGWQ_UY0_fw/viewform Thank you

00:01:06 From George Mulhearn to Everyone: thanks all!

00:01:10 From Liem Truong to Everyone: Thank you everyone!

00:01:11 From Paul Grehan to Everyone: Thanks to all the IIW peeps for organising !!

00:01:19 From Max Stuehrenberg to Everyone: thank you!

00:01:21 From Sammotic Switchyarn to Everyone: Thank you

00:01:22 From Rinkal to Everyone: Thank you everyone!

00:01:26 From ericdrury to Everyone:Thanks!

00:01:26 From Jo Spencer - Sezoo to Everyone: Thanks for staying up Kaliya and Heidi!!!

00:01:27 From Yuji Suga to Everyone:Thanx

00:01:30 From Kaliya Identity Woman to Everyone: http://www.internetidentityworkshop.com

00:01:42 From Ekta Zope to Everyone: Thank You everyone!

Attendee Blog Posts

"A short note about the recent half-day IIW workshop "Digital Identity Across Asia". More discussions and engaged..."

Sankarshan Mukhopadhyay
https://www.linkedin.com/pulse/digital-identity-conversations-discussions-sankarshan-mukhopadhyay/?trackingId=ganTY%2FOLTHSKawkr1EuA%2FQ%3D%3D

Stay Connected with the IIW Community Over Time

Helpful Community Resource

Each week Kaliya, Identity Woman and Informiner publish a round of the week's news from the industry. It is called **Identosphere - Sovereign Identity Updates (weekly newsletter)**

You can find it here: https://newsletter.identosphere.net/ to subscribe

You can support this work via Patreon (yes the newsletter is on substack and we do Patreon)

This work leverages our community blog aggregator that you can follow too.

IIW Community Personal Blog's shared via: https://identosphere.net/blogcatcher/

IIW Community dot.org's in the IIW Space: https://identosphere.net/blogcatcher/orgsfeed/

If you want your blog to be included please email Infominer: newsletter@identosphere.net

A BlogPod was created at IIW - Link to IIW Slack if you want to share/connect with others in the community blogging – https://iiw.slack.com/archives/C013KKU7ZA4

If you have trouble getting in, email Kaliya@identitywoman.net with BlogPod in the Subject.

Other Community Group Work

VRM (Vendor Relationship Management) Mailing List:
https://cyber.harvard.edu/projectvrm/Mailing_list

Credentials Community Group Weekly Call information: https://w3c-ccg.github.io/

Hope See you November 15 - 17, 2022

For **IIWXXXV**

The 35th Internet Identity Workshop
In Mountain View CA at the Computer History Museum

www.InternetIdentityWorkshop.com