IIW Special Topic Workshop
User Experience of SSI
July 22, 2021

User Experience of Self Sovereign Identity (SSI)
Book of Proceedings

July 22, 2021
Online, Near You ~ via QiqoChat

IIWXXXIII Online / October 12 - 14, 2021
REGISTER HERE

www.internetidentityworkshop.com

Contents

IIW Special Topic Workshop
User Experience of SSI
July 22, 2021

Welcome | Agenda Wall | Open Space | **Participants**

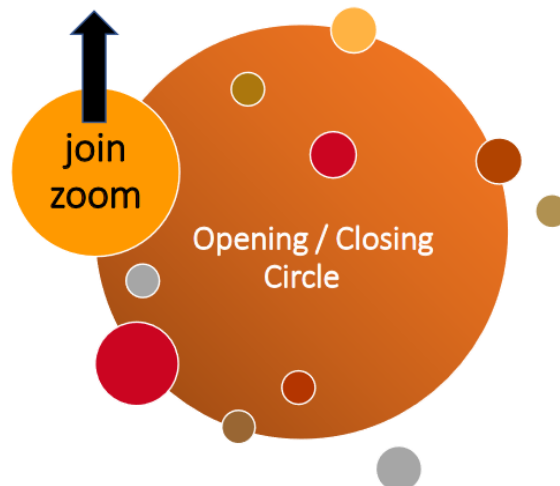**Welcome!** Click the Join Video button at the top left to launch Zoom.

↻ | 🔒 How to Lock Event

Online | Registered | **Map** | Search

About IIW

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 17th year and is Co-produced by Phil Windley, Heidi Nobantu Saul and Kaliya Young. IIWXXXIII (#33) will be October 12, 13,14, 2021, registration will open in mid-June.

<u>Upcoming IIW Events</u>

IIWXXXIII #33
October 12 – 14, 2021
REGISTER

https://internetidentityworkshop.com/

IIW Special Topic Event – User Experience of SSI

This IIW Special Topic event creates the space for User Experience Professionals, Product Managers, Interface Designers, and those in related roles working on decentralized identity or self-sovereign identity applications and tools to discuss, share and collaborate together.

We know there is a lot happening in the industry and we know that just as important to the success of the technology as the "tech stack" is the human experience while using applications built on it. This half day event is an opportunity for those focused on UX to dive deeply into this side of things.

About this event:

IIW Events are participatory workshops where the agenda is co-created by participants the day of the event. We are experimenting with 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.

- Pacific Time: 8am - 1pm
- Mountain Time: 9am - 2pm
- Eastern Time: 11am - 4pm
- Europe Time: 4pm - 9pm London / 5pm - 10pm Berlin

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

IIW 32 Opening Exercise in Small Groups

Each IIW begins with a round table exercise designed to both start the current identity conversations and connect new with long time attendees. At the Special Topic – User Experience of SSI Workshop the prompt questions were focused on the following questions. When groups returned to the main room, they were asked to share what was discussed in the Zoom Chat.

> Name
> Where on Earth are you?
> What is your connection to SSI company/projects?
> What is the Biggest UX challenge we as a community need to solve?

When groups returned to the main room, they were asked to share what was discussed about the Biggest UX Challenge in the Zoom chat:

- Onboarding and passphrase retrieval, general education
- "Teaching" users how much to teach vs hide from users
- Being responsible for your own keys/identity/recovery
- Where can we continue to collaborate on UX across the identity community, across company lines?
- Social engineering - good/bad/how?
- How to encourage users to care about SSI and identity, why it is relevant and useful to them
- Accessibility of SSI across mobile / desktop devices
- Complexity, Metaphor, Mental Models
- How to manage the sense of "overwhelm", especially at scale
- Clarity on all the use cases for identity conversations humans want/need with systems and devices and with each other.
- How to transport ID to user that are not used to technology, How to transport those it to businesses.
- We had really great conversation going, but did not get exactly to the central q. ;)
- To me, coming from the B2C space, it's really a bit pre-UX: framing the value prop.
- Introducing issue-hold-verify roles to un-initiated users who may perform one or more of those actions
- A visual language for this, semiotics and iconography that are universal like the "VCR" play/pause/next/rewind buttons.
- Compatibility between wallets and the amount of them…

Session Topics / Agenda Creation

		IIW Special Topic UX of SSI	
Sessions 1hr Each		**Agenda Wall / Sessions 1 – 3**	
B	Breakout B	What is the complete list of use cases for identity conversations?	Phil Wolff
C	Breakout C	How can we convince real people they CARE about their data agency?	Jonny Howle & Kimberly LInson
D	Breakout D		
E	Breakout E		
2	**Session 2**	**Start Time:** 10:00am PDT * 1:00pm EST * 6:00pm BST * 7:00pm CET	
Breakout Space		**Session Title**	**Convener Name(s)**
A	Breakout A	Is self-sovereign identity a human rights disaster in the making?	Adrian Gropper
B	Breakout B	Requesting information from a user: What does it take to get an answer?	Adrian Doerk
C	Breakout C	Onboarding & Education	John Kuo
D	Breakout D	Design for appropriation	Bentley Farrington
E	Breakout E		
3	**Session 3**	**Start Time:** 11:00am PDT * 2:00pm EST * 7:00pm BST * 8:00pm CE	
Breakout Space		**Session Title**	**Convener Name(s)**
A	Breakout A	How can we continue this work? Overcome barriers? Who is paying for SSI user research?	Phil Wolff

11 Sessions
were called
and convened
by
48 attendees

Notes
were submitted
for all
11 sessions!

Session 1
1A/ A look at a first pass UI for SSI. Its to complex, what now?
1B/ What is the complete list of use cases for identity conversations?
1C/ How can we convince real people they CARE about their data agency?

Session 2
2A/ Is self-sovereign identity a human rights disaster in the making?
2B/ Requesting information from a user: What does it take to get an answer?
2C/ Onboarding & Education
2D/ Design for appropriation

Session 3
3A/ How can we continue this work? Overcome barriers? Who is paying for SSI user research?
3B/ Crossing the desert of integration for issuers and verifiers
3C/ UX of Key Recovery/Management
3D/ SSI +/vs. Marketing & Customer Service

Notes Thursday July 22 / Sessions 1 - 3

Session 1

A look at a first pass UI for SSI. It's too complex, what now?

Session 1A
Session Convener: Mick Lockwood
Session Notes Taker:

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

https://www.frontiersin.org/articles/10.3389/fbloc.2020.609101/full

Standardization of metaphor

Is selling SSI about selling a new type of laminating on an ID Card
STandard set of tools.

20 core areas that need to be thought about and agreed upon
Will accelerate adoption if they can be figured out.
In the real world today we present our identity in numerous interactions

Scalability is an issue.
Different applications hold different types of credentials.
UX to hold different parts of the interaction.

Data specify how credentials are visually shown. Herartio just submitted RFC to Aires about how you present it.
Some might be invisible in the app and working under the hood.

Complicated and

I'd love to collaborate more on the metaphor and mental models in the open! Are there places this is happening already? Lots of +1

Design Pattern Interaction
Variables collectively agreed upon - what do we need to resolve.

Perhaps we can collectively self-organize into some sort of working group, if one doesn't yet exist?
https://github.com/kiva/protocol-sdk-verifier

Chat

Personally, I think SSI is a demo sell, and what gets demo'd is an invention that mothers necessity: something that people see and want immediately, because it's so useful.

What kind of demo do you see as most impactful? I think it's a demo of touchless, instantaneous verification, anywhere - without giving up all your data. An Apple-Pay like experience for proving who you are.

Yes, if we manage to solve all issues so we will have a really open system with no vendor lock-in

One of the bigs could solve this if they don't want to own it all. Alas, this is not how Apple, Google and the others work.

I think there are some very solid ways to convey the value of SSI. Do we even need to convey the hidden ones (e.g. encryption)? How important are they?

I think the fact that Microsoft has released ION but Google, Apple, and FB are highly incented to NOT support SSI is relevant…

Great point on ION, John. A link: https://techcommunity.microsoft.com/t5/identity-standards-blog/ion-we-have-liftoff/ba-p/1441555

What is the complete list of use cases for Decentralized Identity?

Session 1B
Session Convener: Phil Wolff
Session Notes Taker:

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

From https://wider.team/2021/06/21/we-need-to-talk-ux-for-identity-of-things-conversations/

What are the identity conversations people want to have with familiar and strange devices?

Before
- Can you (or a proxy) have a digital identity conversation with me? Are you able and/or willing?
- If you're unwilling, tell me enough to follow up elsewhere.

Getting acquainted
- Tell me a little about yourself.
- What's your name?
- Who are you?
- What do you do?
- What's your history?
- Where did you come from?

About me
- What do you know about me?
- May I introduce myself?
- What may I do with you?
- Could I do more with more permission? From whom?

About the folks behind you
- What groups are you a part of?
- Who is your guardian?
- Who controls you, if not your guardian?
- What do you do with information you collect? What do they do with the information? Who do you trust?
- Where does the information go? Physically, I mean. Does it leave the neighborhood? The country?
- What jurisdictions apply to you?
- Who governs you? What trade, safety, industry, or regulatory bodies?

About your needs and wants
- Who takes care of you?
- If you're abandoned, what happens to you?
- What do you need to survive? To flourish?
- Are you subject to human rights laws? Civil rights laws? Are you more than property?

After
- How can I subscribe, follow, join your circle?

- Would you like to be in a relationship with me? Will you accept my contractual ToS?

Meta
- Who is assuring me this conversation should be trusted?
- How do I report a problem with this conversation or its content?

Triangle of Trust
- Transitive trust. Me, You, and the Third-Parties
- Add: Verify the issuer
- Add: TPM (trusted platform model and hardware root of trust)
- Trusting the network

Simplification and dealing with too much data/alerting
- Personal agency. Human organizing the list of things. Personal folksonomy/tagsonomy.
- Automation. Pattern matching and grouping of things.
- Challenge: ML training without violating privacy principles.

Human Agency for problem relationships?
How do I leave a relationship?
How do I limit a relationship?
Who do I go to for help?
Money layer
https://energyweb.org example for energy grid management. But are there identity UX challenges specific to money and finance?
Offline and paper experiences of SSI?
Do we have common UX patterns for paper identity to work with SSI?
EIDAS digital wallet.

Personal personas (managing groups of my identities by persona and context)

Guardianship roles
Medical power of attorney, delegation.
Automotive ownership (but others own components and services). Vehicle as corporation.
Resources:
- ToIP slack channel - for conversations about healthcare identity interactions. Guardianships, etc.

How can we convince real people they CARE about their data agency?

Session 1C
Session Convener: Jonny Howle & Kimberly Linson
Session Notes Taker:

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

Clarity of data you are about to give up. How to be transparent.
How do we solve education around the value prop of SSI? And make people
Should we focus on the functional value prop of keeping your data private? Not mentioning SSI in messaging.
What does privacy mean? Add complexity of consent. They don't want to think about these new processes. It needs to be more seamless in the context of flow.
How do we move trust from an institution to your personal control?

How do we make people care?
How to have the same level of empathy for people?

Explain the value as this is your personal privacy policy that someone needs to adhere to.
Have strong enough use cases to prove the value proposition.
How do we build wallets that people trust to hold personal information?
How do we make their wallet feel more personal / feel more real?
How does design indicate a better power/sense of control?
Make the risk of exposing your data more transparent (show a level of risk-o-metre).
Privacy paradox: relative vs actual - The economics of Privacy by Alessandro Acquisti.
https://www.heinz.cmu.edu/~acquisti/papers/Acquisti_Beyond_the_Privacy_Paradox_Objective_Published.pdf

How do we solve this:
- More playful UI (better UI and UX). UX copy-writing is crucial. Make the copy human.
- Better terms of service agreements. Less legalese.
- Providing reasons for actions (this is why we are asking for this/why did this fail/why can't I share this). Make every action transparent.
- How does the experience fit contextually into the situation that you need it in?
- Do we add configuration to automatically verify credentials? (set preferences as you use the wallet that learns the way you use it).
- Alerts that notify you before you share a really valuable piece of information (create your own guard rails in preferences).
- Right to be forgotten included in preferences.
- Ability to package a list of credentials.

GDPR - it is a requirement to tell what each piece of information is being asked for.
"If i don't give you this info, what's going to happen'' communication.
https://gdpr.eu/privacy-notice/

Metaphor: Diabetes education.

Session 2

Is Self Sovereign Identity a human rights disaster in the making?

Session 2A
Session Convener: Adrian Gropper
Session Notes Taker: John O'Hare

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

Privacy is a tough topic to get engagement and funding

What are the protocol conversations on top of the now established data models

Adrian: 90% of the funding for the standards work has been from the DHS and BC Gov. And most of the conversation has been about B2B, which is ironic for a self-sovereign topic.

Adrian's recommendation for privacy was not accepted by the DHS despite outreach. The EFF was only willing to talk off the record. No direct involvement wanted. No motives imputed Just saying. Not a detractor of work on verifiable credentials. In fact proud of the work, which is also table stakes.

Next step is to consider the protocol issue on top of these data models.

How do we get community participation?

In the SSI standards community is misdirective because it is all being built by the issuers and verifiers, and not those who would prevent a human rights disaster.

Too much focus is coming from B2B participants because of the incentives. Insufficient critical mass for SSI individuals?

More disciplines are needed at the table to prevent blinkered focus

Is the standards world the way to do this? Is the decentralised model (as per blockchain) a good fit?

ION is an interesting hybrid implementation example being open source and free and somewhat disconnected from Microsofts incentives

Why is SSI a human rights disaster recap, identity has always been abused, how can SSI actually be made personal portable not immutably abusable?

Once you have a chain of custody you're treating everyone as though they're witness at a crime scene. The protocol on top of the data structures are key. Digital slavery at the hands of the digital issuer and wallet specifier.

Elizabeth Renieris's main issue is with blockchain. She has other things to say (I recommend reading her work), but that's the big one.

Once the power to present your information is with users the culture will trend to demanding the information?

Removal of the right to delegate agency is somewhat implicit to the current SSI protocol level

Adrian: the protocol work, funded by the DHS, I characterize as digital slavery. Because, if the sovereign issuer, say government, is able to specify what kind of wallet your credential goes into, and that there has to be a chain of custody between issuer and verifier, that includes a digital wallet, in effect this leads to the same place as SSO: captivity. What happens is that the way these

credentials move is like an ankle bracelet. Yes, they may not have a biometric, or something that calls home, it's still like Aadhaar. Its really easy to get into a situation where every verifier get to control the individual. (Hope I got that right._

If the data models are used in such a way that you don't have the right of delegations to an agent, you don't have real sovereignty or agency.

It's a chain of custody issue that didn't exist in the prior'world

Current standards are a reflection of the funding models and incentives.

Is there an answer? Adrian: the IETF. Rich Authorization Request is the group there to give us hope. adrian and Justin Richer are working on an RFC. There is another group (Grant Authorization??? missed it) that is also relevant.

Rich authorisation requests.

Links of interest / refs
https://docs.google.com/document/d/1Mt1m-fVaSxY6QC3mgHcrNoNH-EnOTRepcwYd9hyjmxM/edit

Adrian: scope creep happened with Aadhaar. See the cruise ship use case above. How do you delegate access to credentials?
Kaliya: we wrote up this use case (missed the name of it). still struggling with possession and control. What about Kiva in Sierra Leone? They have a wallet for everyone in the country.
Adrian: India has indiastack
Kaliya: that sucks.

This is the Chat:
13:07:33 From dsearls to Everyone : Heather, what's the name of your business? Do you have a link?
13:07:46 From JohnOHare to Everyone : I can have a go
13:07:57 From JohnOHare to Everyone : i'm doing childcare concurrently though
13:09:49 From dsearls to Everyone : I'll chat some notes...
13:10:52 From dsearls to Everyone : Adrian: 90% of the funding for the standards work has been from the DHS and BC Gov. And most of the conversation has been about B2B, which is ironic for a self-sovereign topic.
13:12:06 From dsearls to Everyone : Adrian's recommendation for privacy was not accepted by the DHS despite outreach. The EFF was only willing to talk off the record. No direct involvement wanted. No motives imputed Just saying.
13:12:39 From dsearls to Everyone : Not a detractor of work on verifiable credentials. In fact proud of the work, which is also table stakes.
13:12:57 From dsearls to Everyone : Next step is to consider the protocol issue on top of these data models.
13:13:26 From dsearls to Everyone : How do we get community participation?
13:13:54 From JohnOHare to Everyone : ^^ thanks I will move them over
13:14:02 From dsearls to Everyone : In the SSI standards community is misdirective because it is all being built by the issuers and verifiers, and not those who would prevent a human rights disaster.
13:18:42 From dsearls to Everyone : Me: Philip Sheldrake is right that we don't have enough interests at the table; Also, maybe the standards world isn't where to get somewhere with this.
13:19:34 From JohnOHare to Everyone : I would like to hear this too

13:19:38 From JohnOHare to Everyone : thanks

13:19:42 From Mick Lockwood to Everyone : Is this is about once you can you will then be forced..

13:21:15 From dsearls to Everyone : Elizabeth Renieris's main issue is with blockchain. She has other things to say (I recommend reading her work), but that's the big one.

13:24:49 From dsearls to Everyone : Adrian: the protocol work, funded by the DHS, I characterize as digital slavery. Because, if the sovereign issuer, say government, is able to specify what kind of wallet your credential goes into, and that there has to be a chain of custody between issuer and verifier, that includes a digital wallet, in effect this leads to the same place as SSO: captivity. What happens is that the way these credentials move is like an ankle bracelet. Yes, they may not have a biometric, or something that calls home, it's still like Aadhaar. Its really easy to get into a situation where every verifier get to control the individual. (Hope I got that right._

13:26:44 From dsearls to Everyone : If the data models are used in such a way that you don't have the right of delegations to an agent, you don't have real sovereignty or agency.

13:27:13 From dsearls to Everyone : It's a chain of custody issue that didn't exist in the prior'world

13:27:46 From JohnOHare to Everyone : ^^ note taking note: notes are OK to this point but I am off to do childcare. BRB

13:28:01 From Dan Robertson to Everyone : Here's Philip's chapter of the SSI book, "SSI: Our Dystopian Nightmare" https://livebook.manning.com/book/self-sovereign-identity/chapter-33/1

13:29:21 From JohnOHare to Everyone : can we get some links please for the notes?

13:29:28 From JohnOHare to Everyone : i misses the acronyms

13:29:44 From dsearls to Everyone : Is there an answer? Adrian: the IEATF. Rich Authorization Request is the group there to give us hope. adrian and Justin Richer are working on an RFC. There is another group (Grant Authorization??? missed it) that is also relevant.

13:29:55 From dsearls to Everyone : IETF not IEATF.

13:32:29 From dsearls to Everyone : IETF stepped up on human rights, and goes out of its way to invite human rights concerns. it's also not a membership organization, meaning one beholden to corporate contributors.

13:33:26 From dsearls to Everyone : Rich Authoritahzation Request. That's the second group at the IETF

13:34:11 From Adrian Gropper to Everyone : https://datatracker.ietf.org/doc/draft-ietf-oauth-rar/

13:34:23 From dsearls to Everyone : Heather: what are the best practices for companies designing away from sovereign?

13:34:56 From JohnOHare to Everyone : ok, I have noted everything to here but I'm out for now. Thanks Adrian that was really interesting

13:35:32 From Heather Kendall to Everyone : ty, John!

13:35:47 From dsearls to Everyone : Adrian: start with delegation as a way to not lock in the customer. Typically companies look at possession as control. They are always arguing away from separation of concerns. Open banking is a good approach to separation of concerns.

13:37:55 From dsearls to Everyone : If you are going to be inrupt and introduce the next generation of sovereign technology,, you should use an established protocol. Open up, like open banking for payment processing. You can change your controller, your data storage provider. Substituttability.

13:38:29 From dsearls to Everyone : Do not do that, and try to control large parts or all of it, is to create a dark pattern.

13:38:45 From dsearls to Everyone : Heather: what about what's going on with regs in Europe.

13:39:00 From Adrian Gropper to Everyone : https://www.eff.org/deeplinks/2021/06/access-act-takes-step-towards-more-interoperable-future
13:39:05 From dsearls to Everyone : Adrian: see the Access Act in the US. EFF article about it ablve
13:39:40 From dsearls to Everyone : chance of it being passed is slim.
13:39:54 From dsearls to Everyone : business interests ae too strong.
13:41:17 From dsearls to Everyone : What we'll have are four regulatory domains: GDPR in Europe, the US trying to figure out how not to do a CCPA. Asian, with Singapore, Korea, China. Then the giant developing world which have yet to figure it out.
13:41:52 From dsearls to Everyone : These four cultures are each going to come up with a statement about digital ID.
13:42:29 From dsearls to Everyone : Standardizing data models is good, but how it is used in data custody and the rest will be different.
13:42:43 From Joyce Searls to Everyone : https://global.oup.com/academic/product/four-internets-9780197523681?cc=us&lang=en&
13:45:19 From dsearls to Everyone : Joyce: need more clarity on the agency part. we need to see where agency gets taken away from us.
13:47:11 From dsearls to Everyone : Adrian: it's about linkage to possession of control.
13:48:58 From dsearls to Everyone : Look at the protocol work in hyper ledger, aires, Dif, it's tied into ledger work. You need to create a record. 80+% of that work will go to waste because the linkage of possession of control precludes choosing a provider. Precludes substitutability. If the protocol work doesn't recognize separation of control from psossesionj, it precludes self sovereignty: real personal agency.
13:49:13 From Kaliya Identity Woman to Everyone : its not tied to ledger work
13:49:49 From dsearls to Everyone : Mick: there is a sliding scale of credentials from the terribly serious to the trivial, and the mechanisms will shift across those.
13:49:56 From Adrian Gropper to Everyone : Cruise Ship Use Case https://docs.google.com/document/d/1Mt1m-fVaSxY6QC3mgHcrNoNH-EnOTRepcwYd9hyjmxM/edit
13:50:15 From dsearls to Everyone : Joyce: I agree but we don't want the scale to be a slippery slope.
13:51:37 From Kaliya Identity Woman to Everyone : Aadhaar was intended by its developers to be literally used for EVERYTHING
13:52:39 From JohnOHare to Everyone : can someone re copypaste here I have lost history of chat
13:52:47 From Kaliya Identity Woman to Everyone : This is literally the Health Pass use-case
13:52:54 From Jonny Howle_Serto to Everyone : Cruise Ship Use Case https://docs.google.com/document/d/1Mt1m-fVaSxY6QC3mgHcrNoNH-EnOTRepcwYd9hyjmxM/edit
13:53:00 From JohnOHare to Everyone : thanks
13:53:02 From dsearls to Everyone : Adrian: scope creep happened with Aadhaar. See the cruise ship use case above. How do you delegate access to credentials?
13:54:04 From dsearls to Everyone : Kaliya: we wrote up this use case (missed the name of it). still struggling with possession and control. What about Kiva in Sierra Leone? They have a wallet for everyone in the country.
13:54:14 From dsearls to Everyone : Adrian: India has indiastack
13:55:04 From dsearls to Everyone : Kaliya: that sucks.

13:56:10 From JohnOHare to Everyone : yeah I would like to know more too
13:56:31 From Kaliya Identity Woman to Everyone : Here is the health pass use-case - https://wiki.trustoverip.org/display/HOME/GHP+Blueprint+Public+Review+Process
13:56:53 From Heather Kendall to Everyone : Michelle Ghazal, who is working on Kiva Protocol, is at the conference today.

Requesting information from a user: What does it take to get an answer?

Session 2B
Session Convener: Adrian Doerk
Session Notes Taker: Adrian

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

Connecting to the user:
- The point of contact
o Website
o Another App
o Printed or presented QR-Code at a physical location
- Presenting the request as QR code or DID:Comm link

Content of the information request:
- Who is requesting information?
  - Difficult when a direct contact (connectionless)
- Is there already a trusted relationship between holder and verifier?
  - If not the verifier doesn't know who he sends the information request to.
- What information is requested?
- Why is the information requested?
- Does the verifier have the right to ask the information?
- How long will this information be stored? Will it be deleted?
- Does the information need to be verified by a third party or only self-attested?

Answering the information request:
- Actually having the information requested
- What is happening if not? -> Use-case not possible!
- Can I offer a credential with the same content and trust level, which is from another source?
o Where can the user get the credential he:she needs?
- Trusting the verifier
  - The end-user just wants a green check mark
  - Chain of certification/delegation is important for due diligence, but not for the user
  - What happens if one of the parties within the delegation chain has been compromised or their certificate has been revoked?
  - Is a green / yellow / red approach necessary (verified, verified, but not 100 % ok, and unverified)
  - What happens to my credential when the delegation chain of the issuer isn't 100 % verifiable anymore?
  - Putting up an illicit QR-Code at an event - how can we protect you from this?
- Being online or having an offline capability
- There are costs associated: Who pays for that?
- Being able to create a verifiable presentation by myself - without prior information request.

Providing transparency:
- What did I share, when, with whom?
- How can I revoke the right to use my data?
- How can I send a deletion request?
- How can I find out how my data has actually being used?

Onboarding & User Education: How to convey blockchain / verified credential paradigms to non-technical users

Sesion 2C
Session Convener: John Kuo
Session Notes Taker: John & Leah H

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

Our application largely obfuscates the fact that we are using SSI and blockchain, and our target users are currently college undergraduates and high school students in the US. In testing our onboarding, we discovered that there isn't really an understanding at all (of course) around the value prop of blockchain and why for example a 12-word passphrase is required, as well as a PIN for app access (the UX is a mobile app). We had responses like, "Why aren't you just using 2FA?"

The challenge is how do we continue to simplify and obfuscate, while still educating our users?

QR Codes as a solution?
https://www.hpec.io/

PIN or biometric only?
Onboard without passphrase? https://www.diwala.io/
Key rotations?

Custodial vs. Non-custodial?
https://trinsic.id/
https://indicio.tech/
https://holo.host/
https://holochain.org/
https://bloom.co/
https://pocket.asu.edu/

What options to you give to the user (how far down the rabbit hole of security do you let them go?)

An observation by Phil Wolff…
SSI onboarding is like diabetes education. Congratulations, you have a hidden organ, and if you don't carefully nurture and manage it in exactly the right ways, you could lose your sight, your feet, your mind, your life. You must radically change how you live to avoid things getting worse. The only way to know your current condition is to painfully extract blood and go through a three minute ritual. Ten times a day. If you don't care for it, horrible things could happen to you. Some day. Maybe soon, maybe not. The more you know, the more power you have to forestall bad things. There's no cure for this condition and once capacity is lost, it's gone for good. Diabetes education takes days, full of technical jargon to memorize, numbers that don't make sense, and abstract ideas that are hard to relate to. And lots of "motivating" scary imagery and stories.

Business constraints and value props and communication
What's the minimum?
Do you want to learn more?

Identity proof services?

Equity solutions:
Custodial vs Non-custodial
SMS proxy wallet

How do you handle multiple wallets?
Users are confused, overwhelmed, and bored

https://www.lfph.io/2021/02/11/cci-verifiable-credentials-flavors-and-interoperability-paper/

What's the most secure vs. most convenient?

NOTES BY LEAH:
John Kuo
Sponsored by Arizona State University
https://pocket.asu.edu/ à non profit Project* Recovery à whats app prove yourself
Save a key without anything else.

Screenshot and making it not machine readable
QR code based proof

James Ebert—you are giving control to the end user
        Let them decide*

Carmel Kelly à Simple onboarding Process à magic link or password
        Get them on – lock it down. https://www.diwala.io/

Onboarding à DID (how to recover)

James Ebert (Indicio) à Key rotation https://indicio.tech/
        He likes to tell the user à "hey this is what we are doing…" Rabbit hole if they want

Blockchain purity à having to remain in tact

Michael Boyd à give users control over their identity.
Trinsic V2 hosts credentials in the cloud so they can access from all devices
More challenging if you have to use your phone
Good custodial solution now is the best foundation
HSM to store keys but for them they are using a magic link
Private key is being given to them but also stored on an HSM server so they can export the private keys rotat
them and then continue forward
https://www.cryptomathic.com/news-events/blog/understanding-hardware-security-modules-hsms

Celestial: https://holochain.org/ https://holo.host/Some users care more than others à Your organization
needs to decide and create policy. Here is what this means and if you want to learn more à Make

Shares
https://magic.link/

NOTE* only 3% of twitter users are using MFA

Jace Hensley – Bloom à confirmation link in email -Private Keys on device and stored on device, and your account only is on your device but if you CHOOSE to allow password restoration you can do a backup à Create a password à Encrypted file à store on their deivice or anywhere else à new device restore the file à single JSON File that they have to store somewhere à similar to what signal does to store it. Android File system*
They can use multiple devices
There is no syncing
Credentials are stored in the hub- all the real data is stored there
On refresh it downloads all the files again.
Full user controlled SSI More difficult to add features*
Primary users à Focused and interested in SSI Verify different parts of themselves and share those credentials with whomever they want-
Loans and lending
People lose keys from android to android –
iOS keychain they auto got back their Bloom ID back.
Since backup and restore they have stopped seeing the recovery failure problems
They use Accuant for ID verification

John Kuo:
He used to work for an AD tech data tracking history, and the government
FBI approached him - they are also tracking us -
Re Equity à non profit and how to monetize
Non smart phone ways of using the app à public library desktop how to use

James Ebert à custodial arrangement

Michael Boyd àhe worked with Farmer Connect à DIDs directly to farmers in Rwanda etc… no incentive for the gov't to give people access to their identity. They chose to go with an SMS proxy often shared by the whole village. Inaccurate paper receipts. Smart Phone app for Farmer Connect.

Alex Castro à multiple wallets how to fix? Making them compatible.
Lauren D à Same wallet and interoperable
Shared Kaliyas paper on the different flavors of credentials

Credit exchange formats John Kuo is hoping to migrate to a platform like Aries

Michael Boyd à Security model that is most convenient (and as secure as possible) – use cases – covid test result -Link First name last name and DOBà Credential

Chat Log:
10:10:06 From PhilWolff to Everyone:
   Education vs Persuasion? The harder the onboarding mechanism, the more you must motivate them through things and support/nudge at moments of doubt or abandonment.
10:15:52 From Carmel Kelly to Everyone: https://www.diwala.io/
10:18:50 From Celestial to Everyone: jumping kitties @james!
10:22:01 From Michael Boyd to Everyone: https://trinsic.id
10:22:09 From James Ebert to Everyone: https://indicio.tech/

10:22:11 From Leah Houston to Everyone: https://www.hpec.io/
10:22:47 From Celestial to Everyone: https://holo.host/
10:22:49 From Celestial to Everyone: https://holochain.org/
10:23:01 From Michael Boyd to Everyone: I'm also a big fan of https://magic.link and https://app.tor.us/ in the crypto-centric wallet space
10:23:52 From Celestial to Everyone: +1 for meeting people where they are!
10:24:45 From Celestial to Everyone: paradigm shifts can be painful, being empathetic leaders in the world we're trying to create is powerful
10:25:11 From James Ebert to Everyone: Really good thoughts @Michael
10:25:17 From Jace Hensley to Everyone: bloom.co
10:25:26 From John Kuo to Everyone: https://pocket.asu.edu/
10:27:27 From Didier Tisseyre to Everyone: What if the email change for example. E.g.: Changing company.
10:39:44 From PhilWolff to Everyone: "People only use ten percent of Microsoft Word's features, but everyone uses a different ten percent."
10:39:59 From John Kuo to Everyone: ^ That's a good example...
10:44:24 From Celestial to Everyone: I'm also very interested in tech equity, and what it means for education. tech is not a universal luxury…
10:45:47 From Lauren D to Everyone: Also including the ability to use credentials offline
10:46:28 From Leah Houston to Everyone: what about a metamask like wallet

Design for appropriation

Session 2D
Session Convener: Bentley F
Session Notes Taker:

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

(Copy paste from something vaguely related)
"The user experience and security of any system operated by people depends on the information conveyed by the user interface, the response of the users, and the interpretation of their actions.

Unlike with physical credentials or cash, issuers of verifiable data (e.g digital identity credentials or digital currency) rely on software or hardware wallets to interpret and convey information to users in a meaningful way by defining the appearance and user experience of credentials in key moments, such as list views or verification and payment interactions.

While there are common patterns applied to this end (aside from typically inheriting the constraints of card-based models) the implementation details remain at the sole discretion of the wallet provider, resulting in verifiable data having wildly different characteristics across various software, platforms and devices.

This is a desirable characteristic in that it will help drive adoption and use of verifiable data as people are able to choose wallets that provide experiences that cater to individual nuances. However, it is our belief that threads of a consistent user experience are vital to enabling trust, potentially allowing individuals to recognise legitimate digital artefacts across multi-modal endpoints, supporting increased accessibility and driving further adoption."

What is the credential equivalent of wireless charging, where apple has changed the UX by adding magnets. Its still technically interoperable, since android phones can charge (just at a different speed)

Perhaps we need to agree on a standard/core UX that we wish to enforce. A common representation of credentials inside of different UIs. Embed a visual metaphor into the credential so a credential is interpreted and displayed in the way the VC prefers (rather than relying on the receiving wallets to interpret in its own way)
   Physical credential provide the canvas for issuers to visualize what it is like to us the VC, tell a story about the data

When issuers are "the definers" of credentials what is that like?
Control is a big part - loss of canvas.

Major issue in user-experience - verifying credentials
what can we do to get User to use mobile app.
Embed within existing service - using something they

Examples
MemberPass - credit unions
Hearro Applications
Wallet into Authenticator app by MSFT

Able to pull data out of one wallet into another.
- universal wallet data structure

Current paradigm avoid taking data to another place.

DIDComm makes possible.
Totally transparent for user.

Session 4

How can we continue this work? Overcome barriers? Who is paying for SSI user research?

Session 3A
Session Convener: Phil Wolff
Session Notes Taker:

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

Existing forums…

What do we need that isn't here now?
Intellectual property licenses that permit private participation.

Funding
https://shuttleworthfoundation.org/

https://apply.opentech.fund/usability-lab/

https://www.opentech.fund/labs/muchlesser

https://solve.mit.edu/challenges/digital-inclusion

https://id-ideal.hs-mittweida.de

https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/SchaufensterSichereDigIdentProjekte/sdi-projekt_id-ideal.html

https://trustoverip.org

Crossing the desert of integration for issuers and verifiers

Session 3B
Session Convener: Michael Boyd
Session Notes Taker: ?

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

How do we improve the UX for issuers and verifiers?

Users controlling their identity - lots of challenges for individuals.
principles of user-sovereignty.

UX of other parties in credential exchange - primarily issuer & Verifier.

Where are folks at and how do we work together?
"the provider"

Desert of Integration
We talked a little about the UX of issuers and verifiers.
We need interoperability, governance, and adoption tools
Issuers:
- More complex flows, especially around etl
- Need flexible and powerful integrations, simple way to get started
-

w/i Aries ecosystem API can be used with any wallet you want.
Good tooling in space for interoperability.
DIF and Aries doing a lot of work together in the open
Big UX issue - is the interoperability issue.
Issuer or verifier - don't want to worry about deploying and maintaining software standards that are moving quickly - how do we provide open source and hosted options that MAINTAIN interoperability.

Governance as code - as issuer and verifier interact via the holder

What issuers can I actually trust - I know it is an authentic wallet.
How do I know the issuer DID maps to a real entity - retailer or airline.
Trust the provider to maintain a list of trusted entities -
Human element of trust to be at play
Looses out

Governance - how do veriifers (and holders) trust the credentials are from a real entity.
Giving issuers and verifiers adoption tools.

This is only a valuable technology if I can onboard members and employees onto a digital wallet without a lot of friction - begin credential exchange as fast as possible. WE spend a lot of time bootstrapping and onboarding - while guaranteeing user-sovereignty. Beyond interoperability and technical concerns. Product owners and spend a lot of time - user-onboarding for individuals.

How do we get an issuer on board?
How do we get a verifier on board?

Many partners struggle to get their technology integrated into an issuer/verifier system.

VC-HTTP-API Help.
Adoption and interoperability
it is meant to be a standard interface to issue and verifier credential.

issuer looking at a bunch of different verifier - plug and play with any vendor - then they should have a standard interface.

No vendor lock-in
Trinsic as a service provides a high quality service - reliability of platform. We are committed to principles of user-sovereignty - that holders/verifiers have ability to export wallet into another system. Importantly - must be able to run their own.

John Kuo - enterprise software - must go in and set up for them.
Can the integration be framed in the context of an onboarding and system implementation process where various server(s) are provisioned and SDKs provided and integrated with their existing processes?
Existing workflows already on identity issuance - so go in and set it up.
Actually automate the credential issuing process.
Hook into existing data - ETL whenever something updated corresponds to credential issuance.

Part of the whole process -

For the VCI-HTTP-API to work or an SDK that integrates into current systems we need to agree on schema, and how (order, and human readability) it should be presented, so we need standards for every use case correct?

Ecosystem in a box.
Trinsic.

Issuers
Each can go in and use templates for credentials.

import different contexts -

Verifiers can talk about what they want.

Q: How are people not being able to assert.
Configure using @wellknown in website - linking to DNS trust
Some trusted 3rd party like government itself publish list of DIDs currently using.

Interoperability is easiest on Verification side - a lot of consolidation on Presentation Exchange from DIF.

How do I verify a credential from any number of wallets?

Send credentials to my new potential employers.
Can I send them a magic link where they just get the presentation?

a kind of link accessible for a short amount of time.
adding on to magic link idea.
reduce need for verifiers to need to know about verifiable credentials.
proof of covid vaccination - qr code on it - only available on browser for a couple min.
could download into credential wallet.

verification flow looks very similar now.

The UX here is a hard requirement.
We can find security models that work for the use-case while keeping convenience and flow.
That is our aim in what we are doing right now.
That apple pay like experience on
Download - app. Scan a QR code.
will make more complex flows for higher value scenarios.

Every state licencing board - can submit name to boards to see if they are practicing.

Sharing about a use-case around classes between higher education institutions.

Visible to both end-users.
Yes or I just want to transfer classes - all credentials being exchanged.
VPs are shadows of credentials.

Issuers and Verifiers - are THE SAME in some cases.

Where people are interested in verifying are not interested in issuing. They don't want to have a public facing issuer identifier.

Verifiers - are users of some sort of system. Cardea - MedCreds
    click a couple buttons - who they are - what they are going to verify. Not a lot of configuration.

Ability to outsource this to entity their customer will not be upset by.

Serto - search indexes web of people using did wellknown.

Once issuer has their did - in did config file. Anyone can verify credentials issued by that did. Calls Serto search - we do that triangulation and resolve to that domain.
 We have been using that method for small use-cases.

Trying as lighter weight version of Serto App.
http://beta.search.serto.id/how-it-works

Q: Managing Organizational Hierarchy
 National registry
 Different Types of Banks
 Bank Branches

 Delegation of Authority - seems related.
Role Affiliation and title credentials
Can understand within an institutional server.

Zero Trust Architectures - separate authentication/authorization
    VC presentation

Me to Everyone (11:04 AM)
I'm taking notes - would love companions helping -
https://qiqochat.com/breakout/16/hzJxInptrUrNnsYWYGCRTqlaG
John Kuo to Everyone (11:08 AM)
We're also using Hyperledger Indy and Aries...
Me to Everyone (11:10 AM)
this is what ToIP is trying to do.
Does the VCI-HTTP-API help?
John Kuo to Everyone (11:15 AM)
Can the integration be framed in the context of an onboarding and system implementation process where various server(s) are provisioned and SDKs provided and integrated with their existing processes?
Leah Houston to Everyone (11:18 AM)
FERPA
Me to Everyone (11:18 AM)
hahah - she says as an instructor at community college - I am forced to hand transpose grades between Canvas and the 1980's oracle database…we are a long way from hat.
that
Leah Houston to Everyone (11:18 AM)
For the VCI-HTTP-API to work or an SDK that integrates into current systems we need to agree on schema, and how (order, and human readability) it should be presented, so we need standards for every use case correct?
Me to Everyone (11:19 AM)
schema's are different then issuance
what is agreed to is the VC format that folks are focused on JSON-LD ZKP with BBS+
Leah Houston to Me (Direct Message) (11:20 AM)
I guess how do you issue something into more than one type of wallet if the different wallets dont have agreement on the schema?
yes I see
Me to Leah Houston (Direct Message) (11:20 AM)
yes VC format needs to align

schema is data elements inside -

Me to Everyone (11:23 AM)

re: Covid use-case this is work the community just did on how to do this well -
https://wiki.trustoverip.org/display/HOME/GHP+Blueprint+Public+Review+Process

Me to Everyone (11:36 AM)

credentials are not hashed onto blockchains in SSI

Jace Hensley to Everyone (11:38 AM)

@kaliya I'm under that impression as well, but some co-workers are certain there's use-cases where the VC should be "anchored" via a hash on some sort of chain. I'm still on the side that that's not needed

Brian Richter to Everyone (11:38 AM)

do they have any examples @jace?

Me to Everyone (11:38 AM)

Credentials should not be hashed and stuck on a blockchain(or in a merle tree)

Jace Hensley to Everyone (11:39 AM)

Mainly a known timestamp that the issuer doesn't control, but my thoughts are if you trust the issuer to put valid data into the VC you should trust the VC's timestamp

Me to Everyone (11:39 AM)

its not needed - you need the DIDs of the issuer to do the cryptographic verification of the proof it has not been tampered with.
especially if you are doing selective disclosure things - the hash of the whole thing is USELESS

Me to Everyone (11:40 AM)

and with VPs each time you share it is different and DOESN'T match the hash because the actual signature isn't shared.

Leah Houston to Everyone (11:40 AM)

DID's are anchored to blockchains VC's are issued and held and not visible unless the holder allows permission. IMO that permission should have user controled limits (time metadata access)

Me to Everyone (11:41 AM)

Verifiable Presentations are proof of holding a VC but not the ACTUAL VC - only the holder sees/gets that

Leah Houston to Everyone (11:42 AM)

Yes and IMO - each verifiable presentation should have only what the holder wants it to have in it, (what the verifier is requesting if the holder agrees)

Julia Celiker to Everyone (11:48 AM)

If companies and organizations already have a workflow in their software. They might want to add another system on top.

Adrian Gropper to Everyone (11:48 AM)

https://docs.google.com/document/d/1Mt1m-fVaSxY6QC3mgHcrNoNH-EnOTRepcwYd9hyjmxM/edit

Julia Celiker to Everyone (11:49 AM)

not!! Might not want to add

Lauren D to Everyone (11:49 AM)

^ Julia. This is a challenge we encountered

Me to Everyone (11:54 AM)

We have 5 min left until Closing Circle.

Bruce Conrad to Everyone (11:55 AM)

Link please Jonny

Jonny Howle_Serto to Everyone (11:57 AM)

Here is the spec: https://identity.foundation/specs/did-configuration/

Bruce Conrad to Everyone (11:57 AM)

thanks!

Lauren D to Everyone (11:58 AM)

Has anyone encountered use cases surrounding delegation of authority?
Jonny Howle_Serto to Everyone (11:58 AM)
http://beta.search.serto.id/how-it-works
http://beta.search.serto.id/domain/consensys.net
^Thats a search result for entity that has implemented the standard
Leah Houston to Everyone (12:00 PM)
Thanks Jonny - is this a spin off of UPort?
similar brand identity…

UX of Key Recovery/Management

Session 3C
Session Convener: Jonny Howle
Session Notes Taker:
List of Session Attendees:

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

Social Recovery
- Argent implemented in production
  - Uses Smart Contract
  - Could be collusion risk
  - Ability to get locked out of wallet because all of your delegates are locked out too
- Should Social Recovery be the root recovery method?
- Shamir Secret Sharing may be better for off-chain recovery that gets around privacy problems of on-chain social recovery

Distributed Recovery
- Should we drop the term social recovery and use distributed recovery
- Distributed recovery is like social recovery but isn't purely about sharing pieces of keys with other people, but with other institutions, devices, etc
-

Key Hierarchy
- Seems like agreement that the future looks like one where users have multiple keys
- What is the relationship between these keys?
- More intense/labor intensive as you move down your hierarchy of keys to the root key

Memory Palace/Gamification
- Seed Quest was an attempt at gamifying the recovery process where seed phrases are mapped to actions taken in a game
  - Idea is that it will make your key easier to remember by forming a narrative around the key content

Fuzzy Encryption
- questions around if this maintains entropy/security
- idea is that you can reconstruct a key from subset of unordered seed words from a set
- Haven't seen it in production yet

Biometrics
Agree that biometrics are tricky but that there might be a role for them to play in the recovery or security of shards

SSI +/vs Marketing & Customer Service

Session 3D
Session Convener: Doc Searls
Session Notes Taker: Celestial Hanley
List of Session Attendees:

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

Need consistent messaging and engagement with users from marketing, product interface, customer support, etc.

Enterprises push customer service onto the customer and make them manage everything, this is painful for users and inhibits adoption of privacy-centered technologies.

Need one streamlined way to deal with everything, like how we use a credit card or cash--this will unburden marketing, customer support, etc. of having to manage the various parts.

Conversation is social lubricant, yet machine processes don't welcome conversation.The frontier is the meshing between the machine mental model and the human mental model, and what are the metrics that give you humanity in a machine system?

One idea is that SSI has to work at the tacit level; a new habit structure has to form

Heaps of complexity--between designing processes and interfaces, as well as between the communities doing that building and designing. Membranes and language patterns between communities--we may be talking about the same thing but using different language.

Closing Circle – As a result of attending Special Topic UX of SSI

*** Please complete the sentence: As a result of attending UX of SSI …. *****

- I don't feel so alone in facing the design challenges of SSI :-)
- I have more feedback and ideas to share with my team than I can currently manage
- I have been re-energized………..
- I was given a chance to connect with others who care about the same problems that I do
- I believe there is the opportunity to execute some structured research on a number of topics that I do not have the bandwidth to tackle myself.
- Met some interesting people and encountered some great ideas
- I have even more bloody questions to answer… 🙃
- As a result of attending UX SSI, I am more committed to UX for identity of things.
- learn and know more about the world of SSI and meet people with different points of view
- I didn't get many concrete answers but lots of ideas to reach them and share in a future IIW!

Resources for Next Steps and Continuing Conversations

An Accessible Interface Layer for Self-Sovereign Identity

Leah Houston: Any independent designers in the audience who want to potentially work with us (HPEC.io) please reach out @LeahHoustonMD and Leah@hpec.io

Maybe we could use open collective?
DIF Product Manager Community of Practice
Human Experience Working Group at Trust over IP

Happy to answer TOIP Human Experience Working Group - kimberly.linson@randasolutions.com

   Hyper Island

Jonny Howle_Serto: I wrote this about social media and how we can address some problems with our SSI tech. Would be happy to contribute to any other ongoing conversations around the topic

Stay Connected with the IIW Community Over Time – Blog Posts from Community Members

New 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/

As a follow up to the session 'Let's Bring Blogging Back' an IIW Blog aggregator has been created here: https://identosphere.net
If you want your blog to be included please email Kaliya: kaliya@identitywoman.net

A BlogPod was created at IIW - Link to IIW Slack –
https://iiw.slack.com/archives/C013KKU7ZA4
If you have trouble getting in, email Kaliya@identitywoman.net with BlogPod in the Subject.

Planet Identity Revived ~ @identitywoman & @#InfoMiner cleared out & updated Planet Identity (see links below) you can support the work here:
https://www.patreon.com/user?u=35769676

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/

Hope See you October 12, 13 and 14, 2021

for
IIWXXXIII Online

The 33ⁿᵈ Internet Identity Workshop

www.InternetIdentityWorkshop.com