! NOTES NEEDED !

1. **Please scroll down & add:** (a) name of Notes-taker(s), (b) type notes directly into the body of this document.

2. **Save relevant "zoom chat" & Clean Up *before*** pasting into the body of this document.

3. **Share any screenshots, slides or photos of whiteboard work in your notes - If you are sharing a slide deck or PDF Doc please put it up on the web and provide a link to it.**

    IMPORTANT: **This google doc page will be accessible through Monday April 26th.**

    After April 26th you can download the IIW Notes Form here. **Record & Save your notes as Word.doc;** then, **submit via email to:** iiwnotes@gmail.com with **Subject Line of Email:** Session # (1 - 24) & Meeting Space Letter (A - P) & Session Name. Thank You!

****

Day 2 / Session 14 / Space M

Session Title: Ceramic, SkyNet, LoRa, IoT.low bandwidth & Memory, Distributed Network. Managing Schemas, DIDComm, and V.C. in Context

Convener: Brent Shambaugh

Notes-taker(s): Brent Shambaugh

Tags for the session - technology discussed/ideas considered:

Discussion notes, key understandings, outstanding questions, observations, and, if appropriate to this discussion: action items, next steps:

From memory:

I recall that Joe suggested simplification. I may not need to use ceramic and I may not need to use LoRa. I may not even need a blockchain or ledger. I may want to exchange public keys with friends to start out and use did:web.

Kim commented about her experience with BTCR. It was a great discussion. Unfortunately, it was not recorded.

When Brent mentioned a hackerspace and IoT use case using verifiable credentials to access machines that one had been trained on, Kim liked the idea.

Brent admitted that this was an exploratory project and there currently were no customers. Kim and (Joe) thought that working on a project was a good way to meet people.

Brent found it to be a productive way to learn about the technology. He admitted that he had not implemented verifiable credentials or completed a did method over ceramic. He admitted that he had only recently learned about the size issues of verifiable credentials on embedded devices from Mrinal from Ockam. He also mentioned that there was an earlier IIW session that talked about the size limitations of Lora: 200 bytes for LoRa and 150 bytes for LoraWAN. The title was similar to " IoT swarms, communication in bandwidth constrained environments".

Joe questioned why LoRa was used. Brent said it was legacy and the project originally started out through a suggestion from a friend to investigate LoRa and drone tracking (to satisfy a potential FAA regulation). He claimed to be unsure about it. He knew that the hobbyists had complained.

Joe suggested that other protocols could be fine, and there was a way that he recalled that ESP32 devices could form mesh networks (out of the box).

Then came discussion of OpenWRT. Brent thought Joe meant (wireless access points? softtAP?) with ESP32.

Discussion of did:web came up. Did:key was thought of as a good way forward (IIRC). There were 3 things that joe mentioned to do, starting with authentication.

Mike Lodder was championed as a good person to talk to.

Here are some notes. They are raw, or as closely as handwriting could be read, with minor spelling corrections:

Use CBOR-LD see order at 10x compression .. boilerplace to very small data.

other non-linked data solution Mike Lodder ... mentioning low bandwidth

Trying to use cryptographic mechanisms just hashes to secure the provenance to see how the verifiable credentials also in context of very high bandwidth application ... need an app

Think about 3 Different Interactions::
+ Bandwidth constrained device. How do you onboard?
+ How do you authenticate...use DID

From authentication storage bootstrap a shared secret .. bootstrap then negotiate like a DES shared secret on the channel depending on the session. that is a cache message issue. just authenticate like a session cookie
over ssl.

+ Use JWT ... negotiate a ...the JWT is algorithm agnostic
-----
specific implement
---
short lived credentials might help you. Bubble passports....fill out application 4 hows to get in....in 4 hours get online
----
High bandwidth ... not in custom...offline don't let you use your phone...only lives for 4 hours...

use ... did:web to resolve that page...using own page ...that one ... in more details...in general update the webpage to update the keys...
tend to be not recommend for a subject of a credential..to work long enough if the domain is stable....don't mind ou if encountered claim related

same thing

getting started....with did:key

did key generates the

3
onboarding --- could have them . give the public key (perhaps over e-mail if I recall)
authentication
transmission

----
another huge...purely...did:web
huge translation did:web...move over...widely used implementations
IoT...list of heuristics for DID method....free must be implementation...
no bespoke blockchains involved...did:web worked just fine....just decided...
before ion before a month ago... sidetree stable now in did limitation no support
for rotation...use that out educational pilots....key get lost rotate...the 1st use case...
public key w/ device...maybe...did associated with friend...did

the public private symmetric

purely generative did method did;key for bootstrapping
system find...

how open is your system....

20,000 decided
I'm device #27

most applications don't need all of that...not third party devices....
----
closed on ...device....with public key

Another chip using OpenWRT...so much time doing mesh network...experiment...

Ockam involved in DIF...some of

Mrinal...super smart making contribution

MIT OpenCourse Ware....BlockChain
moving new SEC Char
sign up...discuss topics

look up to what a did document at a specific time ... not not all did
methods point in time lookups ... b/c the did resolver ... only thing guaranteed the latest version

we never resolved the semantics of dealing with time

some use cases...inappropriate historical analog merit...
--no longer current ... comprised...
long term identifier subject

what is did:web a method spec ...
a web byte ...2 forms...
did document under domain
---

did document for ...something
trust one is you know to look there
you can but did document threr...
starting did document...put in a github page
----
registry...use did:key ...know claims associated...up to date
list with keys...within a number of your friends make update before
the other coolin thing exploratory
thing as well...good opportunity..
doesn't have to use peer blockchain
must not doing...maturity not
boy there.... threat model not there...use did:web update
web--page...

these are components...and non work together..
feel free to cobble...don't feel
I've got to note didish
----
once a year ago...specific use
case...did in credential....update keys
2 things issuer and recipient

wouldn't working security badges that would require...depends
on how much worth it..
----
so much stuff, fun with did method

----

2 different formats .... get public key ... get public key now risk that someone got the public key ... for mil spec ...103...

--

didn't ---these things ---ability to use---but over kill

P2P how do we fix web of trust. figuring correct public key ... if you can trust you have a public key. MiTM.

Grand visions didn't need a mesh network.

Use local WiFi most use cases....

Broadcaster ...gears ESP32...