Figuring out Verifiable Credentials Exchange - Combining Bloom, Aires Protocols, Presentation Exchange into a Unified - Killer Whale Jello Salad

Thursday 22H
Convener: Kaliya Young
Notes-taker(s): Kaliya Young

Tags for the session - technology discussed/ideas considered:

DIDComm, Verifiable Credential Exchange, Aries Protocol, Bloom Protocol, Presentation Exchange,

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

Slides to complement this document - https://docs.google.com/presentation/d/1t4o6AXclqR7SqhGCbIJKVtYxh4fm_5mGT11MBx9K95c/edit#slide=id.p

This session was the 2nd in a series - the first one was Day 2.
"Credentials Exchange - Figuring It Out - (Jello Bowl Death Match?) [please link to these sessions in the wiki version]

The third one was in the last session.
"More Killer Whale Jello Salad...figuring out how credential exchange can harmonize. ← this one has the outcomes of the work and next steps artilcuated. [please link to these sessions in the wiki version]

State a vision or goal - dream scenario.

Presentation exchange across trust zones (relative to the VC-HTTP-API) - new way of doing it? How much influence to ma
Opportunity to make next version support - Aries Ecosystem and BBS+
Future
Vision - everyone has one way that is documented to move BBS+
Demonstrating interoperability over HTTP

Do it right - interoperability - would have vendors from Aries in there passing the tests.
Lets make interoperability set go up - make API evolve to make it work.

Orie is working on a code example here:

- https://github.com/OR13/waci-didcomm/blob/main/test.js

- Related to: https://github.com/hyperledger/aries-rfcs/blob/master/features/0510-dif-pres-exch-attach/README.md#request-presentation-attachment-format

Plz help.

Orie's summary of where DHardman/DIDComm-community is alignment-friendly

- Transport = URI-friendly (over HTTP for now/this version of CCG-SVIP interop tests)
    - Sam C: transport over websockets as an example of how to narrow scope further to what's easiest to align
- Envelope = didcomm [v2] compatible (JWE)
- Payload = json
- Easiest way to align interop testing FOR NOW

No Negotiation for V1

Presentation
Two message?
It is Is a two message flow if you constrain it.
(to be clear) it is not request/response - it is two message.
Reasons for complexity - get down to two if you want to start there.
Cryptography may pass - but business case won't.

VC-HTTP-API (VHA) - has no holder interaction.
Discussion of expanding to VHA - do this instead of that (expanding)

Look at DidComm messaging

What parts of the presentation exchange can we cut.

"Presentation-Exchange has a large surface area - we should agree on the subset we want to support for AIP 2.0."

What key parts do we need to drive attention to for a simple 2 message spec.

VP request spec - assumes JSON-LD - includes payload
Initially proposed - through over HTTP and get it done.
Do it better and have it be better.

Seen another way of doing things.

Functionally - similar to GNAP

What comes back from here is a presentation - ??

Magic - request multiple credentials at the same time - allows sending multiple at the same time.

David - asked a question about Schema URI. - pointer to a policy? What I get what I want. URI is intended to - what is the primary resource indicator - winno down the list.

Fetches policy - policy registry -

DIDComm HTTP transport
JWT
LDP

Posted in previous session, but again, here is some discussion:
https://github.com/w3c-ccg/universal-wallet-interop-spec/issues/84

Do you have right format right keys.

DIDComm HTTP - what is there what do need to build.
https://identity.foundation/didcomm-messaging/spec/#https

Things i don't see here that I expect to see.
HTTP end point - opinion of router itself.

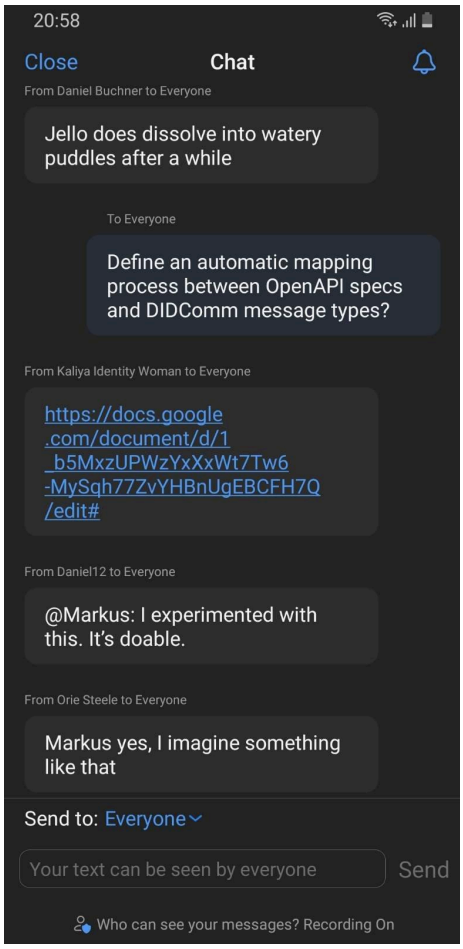
Doesn't look like Rest - Message oriented HTTP.
Fits in a swagger.
Messages that are getting created.
Possible open API specification 3.

DIDDoc Service end-point doesn't have an option about scope.
Routing key seems something cut for first version - web accessible end point can get wavy without messaging key - apps on mobile devices will need it.

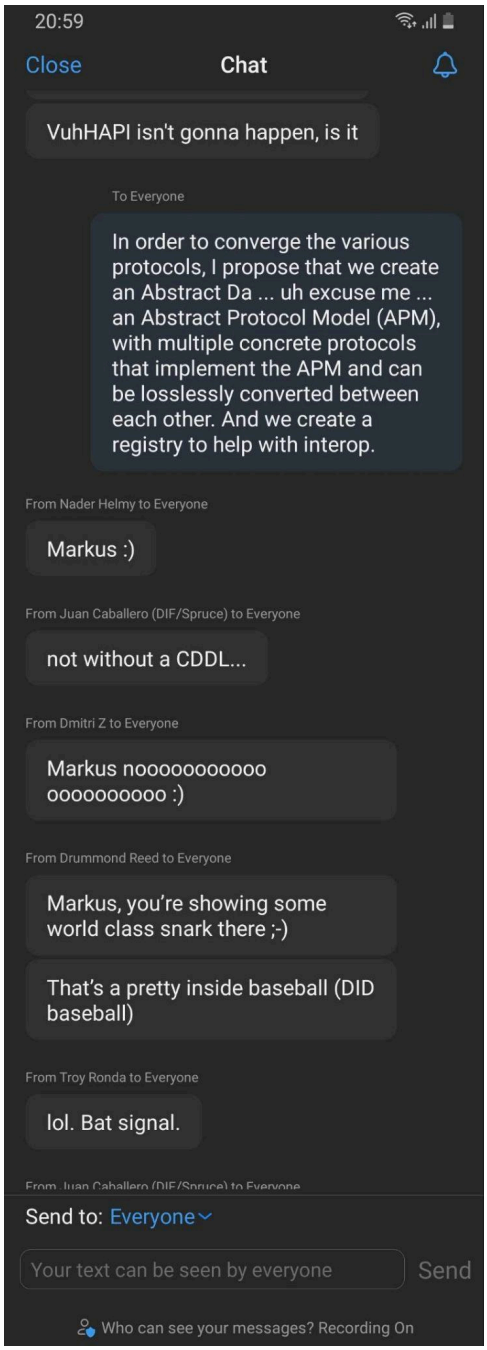
In case where mobile is wallet do I need a mediator.
Mobile agent or web wallet not have an end-point - yes need mediator.
If present to wallet that is a mobile application - mediator pass to mobile application.

Markus - structure of service end points.
Rest patterns.
Paths/routes of URL
DIDComm message type map to REST-like HTTP URL paths (e.g.for issue, present, verify, etc.)

Chat: Define automatic mapping between OpenAPI specs and DIDComm message types



Joke: Define an Abstract Protocol Model (APM):



2 ways around - place constraints on the protocol that is allowed.
Declare a new protocol?
VHA - VCI- HTTP-API

Is there a “setup phase” that we can skip?
InteropAPI

How does Bloom feel?
Cool to see it be used - excited to be a part of this effort here.

Does Authorization have anything to do with it?

What are the animals we can see from our boat deck. OpenIDConnect - and SIOP
DIDComm + Aries FRCs together + Bloom proposal

VC-HTTP-API and Aries Alignment.

Coupling certain credential formats and exchange.
Yes: We talked about DIDComm v1 only really supporting ZKP CLI
And OIDC only really support JWT

DID privacy -
One service end point +/- mediators.
If there is going to be only one? To a messaging protocol or an authorization protocol?
Answer: Let GNAP, HUBs, and Agents fight that out in their own session
Answer: Sake of narrowing things down - DIDComm (has a service endpoint definition - but could
Orie I think service endpoints are not needed

Anil Question:
What are the things that are defined and articulated in the envelope format?
Answer:

- JWE - structure inside
- Each message has a message type - attributes you can expect to look for
- Message ID
- Threading mechanism
- Timestames that can be included.
- Message - content is subject to the message type as defined.
- Payload is JSON - can be JSON-LD? - Yes JSON-LD non-conflicting.

  Request body in VHA - is just JSON but can be JSON-LD - request response format is VHA - does not assume JSON-LD.

We have put a stake in ground with JSON-LD - make sure we are not losing anything or compromising anything - we are not.

Anil Question: Hard requirement - around selective disclosure - pairing based cryptography BBS+ - does anything you are proposing prevent that - within movement between?

Answer by Orie: Issue-movement- holder whole point is to enable this - for both sides of the community - Aries - able to support both of them in both communities - and prove interoperability -
Seconding what Orie said: Intentionally defined to be agnostic - to payload - new definitions might be needed.

Anil Question: Perspective from organizational perspective - diversity of types of wallets - web based ones, agent based wallets. Does this help - providing a common pathway used by both.
Orie: this supports that vision in particular if adopted will allow interoperability testing - web wallets, backend services and native wallets (apps).

Anil Question: we know how to manage REST based APIs - if we go down this path - do we need to make this special - can the current generation of capabilities in an API gateway support something like this.
Sam: you can use an API gateway - each of the Rest calls to a different URI - know the URI to make things happen in - didcomm recipient has an encrypted - so it knows the type of message. Not make internal semantics visible - some of the features - won't work the same way.
Stephen says: - it is fully aligned with an API gateway - you can't see the inside the message. Lots of routing you can do with it - we have found in enterprise environments we are very aligned with it. Backend side of controlling is aligned.

Anil Question: How do people define API - HTTP proxy headers - also point of security enforcement. Does it take away with existing API authentication mechanisms like OAuth - mutual TLS - impact to current API security model.
Orie: - transport level security concerns and message level security concern - can still apply transport level security that you can - do now.

Adrian: Anil's last question - can we factor out by design the encryption part form the payload part - between UMA1 and UMA2 - mutual TLS connection.
Jacob: seconds. Hold message level encryption and hold line on this - big issue is key distribution. What ends up happening keys need to scale horizontally. Or you decrypt at boundary - message level format anyways.
Is there a way to separate payload contents.
Cost to have interop with message level security folks - worth hightented friction - to have common interoperability - arguing level to turn of message level encryption is arguing to not use DIDComm
Cost of processing spam - becomes and issue if we do this wrong. IT is not just Jacob seconding. Not just question about factoring it out

Cost hast be on sender.
Lots of ways to deal with it.

Anil - I sympathize with question Jacob asked and answer that Orire gave.
The flexibility of making choice should be given to enterprise - so they choose
Surviving multiple hops.

https://github.com/hyperledger/aries-rfcs/blob/master/features/0510-dif-pres-exch-attach/README.md#request-presentation-attachment-format

https://specs.bloom.co/wallet-and-credential-interactions/

Skip over bloom spec.

- RFC-454 parties present a proof
- Agnostic about actual format.

Important parts of the protocol - what format you want is in an attachment.
You can provide multiple attachments - request things in multiple formats
You have the option of responding in different formats.
Messages - that go back and forth and messages that respond with different formats.

DIDComm v2

Work Item within DIF right now - envelope format with some other opinions we may or may want. Daniel Hardman gave vision - of parts that are done - leaving behind parts not done.

- DIDCom V2 Envelops JWEs (a standard that exists)
- Aries RFCs for payloads that go in JWE envelopes.
- Send envelopes over HTTP as a starting point