OIDF DCP meeting - 19/04/2024

Attendees list:

- In-person
    - Joseph Heenan
    - Mike Jones
    - Oliver Terbu
    - Gail Hodges
    - Naohiro Fujie
    - Shigeya Suzuki
    - Niels Flensted-Jensen
    - Kristina Yasuda
    - Torsten Lodderstedt
    - Lee Campbell
    - Rick Byers
    - Dirk Balfanz
    - Tobias Looker
    - Paul Bastian
    - Helen Qin
    - Pedro
    - Gareth Oliver
    - John Bradley
    - Marcos Cáceres (observing)
    - TBD
- Online
    - Andy Lim
    - Brian Campbell
    - Christian Bormann
    - David Chadwick
    - Dima Postnikov
    - Gabe Cohen
    - Hicham Lozi
    - Jin Wen
    - Rajvardhan Deshmukh
    - Sebastian Bahloul
    - Sudesha Shetty
    - Victor Lu
    - Andres Olave

Agenda:

- Browser API
- Query language
-

Browser API

Torsten presenting https://github.com/openid/OpenID4VP/pull/155

Clarified that the wallet needs to understand the request, not the platform necessarily but it depends on the design of the platforms.

At IIW, Google/Apple showed a demo of a CTAP Hybrid flow for a cross-device credential request flow. The API is not available yet because it needs small modifications to CTAP. Demo was done Android to Android and Chrome on desktop to iOS.

Clarification on encrypted response that the ephemeral key of verifier is included in the request and the wallet uses JARM to encrypt the response. Clarified that PR 155 does not change that model.

The WG is asked to review PR 155.

Query language

At IIW, a session was hosted on “Suggestion for PE simplification”. Hosted by Kristina, Tobias and Oliver.

Kristina presenting and summarizing the IIW session.

Useful primitives of PE will be reused but certain parts will be replaced such as JSONPath.

Input descriptor changed to contain “format” parameter and “format” parameter value denotes specific parameters in the input descriptor.

For example, mdoc has doctype parameter, SD-JWT VC has “vct” parameter. Certain parameters are shared across formats, e.g., claims parameter but specific properties can vary per format.

Discussion was on how to encode alternative options in PE, e.g., alternative_claim

DCP WG should provide feedback on:
- Requirements included in the IIW slide deck (also on OID4VP github)
- Are members comfortable with the compromise and the direction of this work

Discussion:

- Where the changes that this work entails is happening.
- Discussion on longevity and identified use cases. It was noted that we don't have all the requirements that we will need in the future but the proposal has extension points such as credential format and even input descriptor (if required) that will allow us to extend the syntax as required.
- Positive feedback from the room on the proposal and the solution is pragmatic.
- Browser API does limit how feature negotiation is done in the future, so simplification is better.
- Discussion on filtering based on the claim value
    - It was noted that the presented model is extensible to support such use cases but it has certain challenges, e.g., wrt privacy and user experience/consent.
    - It was noted that the proposal does not support claim value filtering but it can be done via extension points if required.
-

DCP WG is invited to provide feedback on the proposal in the following issue:
https://github.com/openid/OpenID4VP/issues/144

Algs vs vp_formats_supported

Torsten presenting https://github.com/openid/OpenID4VP/issues/53

Discussion on where to include the parameter since there is some redundancy: input descriptor vs request parameters (i.e. client_metadata). Torsten proposed to have this information only in the input descriptor and not as dedicated request parameters (i.e. client metadata).

Tobias:
Cryptographic related parameters might not change on a use case/request basis since it is deployment specific. Similarities with credential formats which would not change that are generally supported by a verifier. In favor of using client metadata.

Torsten:
Countered that the German eID model might select crypto algorithms per use case, e.g., HMAC. There might be cases where RPs might decide to support HMAC for PIDs but not for (Q)EAA.

Tobias:
Concerns raised on security of the input descriptor approach, e.g., downgrade attacks, especially if unsigned requests are used.

Torsten:

Input descriptor is transmitted in the same way as the request parameters, so security concerns would not change depending on the model.

Paul:
In favor of the input descriptor approach.

Kristina:
It has to be discussed how input descriptor approach relates to client metadata obtained from other sources, e.g., OpenID federation.

Torsten:
In favor of having a defined hierarchy of where the information can be pulled from but all should be supported if required:

- Client metadata from other sources
- Client metadata or presentation definition in the request.
- Input descriptor

Discussion:

It was discussed whether we should hold on to the client_metadata parameter in the request (introduced by OID4VP). Parameter is mostly only used for transmitting ephemeral keys.

John:

If browser API matcher does not have a sanitized way of getting the client metadata, we will probably have to keep the parameter in the request.

Kristina:

Asked John about request parameters when OpenID federation is used that is required by matcher.

John:

Can start with a minimum set. ALl information that is normally to be referenced probably has to be in the request. Probably more than one trust chain, so probably more than one anchor. Leaf is needed and probably enough for the matcher but wallet might need other things. What matcher needs is self-asserted version of what the wallet needs to verify. Simplest approach would be that passed in via the request.

Mike:

One option of doing it would be simpler and better. Counter-productive to have algorithms supported defined in the request.

Could introduce another PE feature dependency that is not necessarily wanted.

Torsten:

Client metadata was introduced by OID4VP and we could move it to the input descriptor.

Mike:

OID-protocol approach is to put that information in the client metadata.

Kristina:

Noted that the goal is not to replace PE primitives.

Tobias:

Likes Torsten's proposed hierarchy of where this information can be propagated to the wallet, ie. client metadata, request, input descriptor.

Torsten asked to provide comments on the issue.

(note taker could not include all discussions on this topic)

Client_id_scheme security

Issue raised by Daniel Fett and Joseph presented slides that were presented at OSW2024.

Presented one potential option to solve this issue is by prefixing client_id values where used with the client_id_scheme.

Issue was clarified that all messages have an authenticated sender or authenticated recipient. With client_id_scheme introduces an ambiguity.

Concerns were raised on pre-fix approach on overloading "aud" parameter value in the response and "iss" parameter in the request.

Discussion on other options that have the same function as client id scheme to address this issue.

Discussion on fallback mechanisms in the request for identifying the client.

Transaction Authorization using Credential Presentations

https://github.com/openid/OpenID4VP/issues/156

Kristina and Torsten presented the use case - **authorizing** doing qualified signatures using VP.

Design document at
https://docs.google.com/document/d/1E_UlB3fh9zbWiPrzFThEnt69hYN60CWk/edit

Concerns that this proposal is adding authorization to a place (presentation) that was just used for identification
The relation of this feature with payments and device binding was discussed. Comments will be added to the issue.

The credential can be any credential. It doesn't need to be the PID.

The relation to dynamic credential request was mentioned (i.e. presentation during issuance).

There is a complex intersection between the proposal and payments confirmation. Also, this introduces a change in the trust model, namely that the wallet correctly renders this extra authorization information to the user.

Discussion if the signed authorization should be inside the VP token or on a separate token.

Suggestions to use the work in the payments specs on the authorization schema.

FYI: some devices support secure rendering by the secure enclave and the inclusion of that information in the signature.

Consensus that mechanism seems useful for both qualified signatures and also for payments.

VCI: merging credential / batch / deferred endpoints

https://github.com/openid/OpenID4VCI/pull/293
https://github.com/openid/OpenID4VCI/issues/167

Paul Bastian presented the proposal in https://github.com/openid/OpenID4VCI/pull/293 for the batch endpoint.

A suggestion from IIW was also presented, where we can remove the credential batch endpoint by adding the ability for the normal credential endpoint to issue multiple credentials, associated to the same credential configuration and data set, but associated with multiple different keys.

Kristina clarified that the batch endpoint doesn't currently have partial failure: they all succeed or they all fail.

There was also a discussion about making a breaking change to the regular credential endpoint or use polymorphism to allow both the current request schema and the new request schema allowing for multiple proofs. There wasn't consensus on the usage of polymorphism.

No decision was made regarding the removal of the batch endpoint.

Suggestion to do the batch endpoint polymorphic, using the same design that we want to apply to the regular credential endpoint.

VCI: authorization_pending

https://github.com/openid/OpenID4VCI/issues/60

Security concerns were raised previously about this feature, namely because deferred issuance can handle most of the use cases.

Request for implementers to add information on the issue about usage of this feature.

No decision was made about its removal at this point.

VCI: Mechanism for notifying the wallet about certain events

https://github.com/openid/OpenID4VCI/issues/300

Oliver Terbu presented the issue above and the motivating use cases. Potential solutions can be based on OIDF Shared Signals.

Question about why is the issuer sending the signals to the wallet and not the other way around, since there are mechanisms for credential status.

Suggestion to also look into the other direction, where the wallet provider also sends signals to the issuer. Proposal to extend the notification endpoint for other types of signal.

It was noted that this new interaction model, with signals from the issuer to the wallet, introduces new security and privacy issues.

It was also noted that the push model cannot be completely relied upon and the pull model is always needed.

Consensus that this is a useful feature, however the requirements need to be agreed upon and a concrete proposal based on those requirements needs to be made.

VCI: review of issuance flows and credential_identifier

Paul Bastian presented all the currently existing variants for authorization requests and credential requests.

Agreement that there is opportunity to simplify the current design, namely by making credential identifiers mandatory on token response, when RAR is used, on both grants.

VP: plan to do a implementers draft 3

Question: should we hold ID3 until the browser API and the query language changes are added.

Mike Jones suggested adding the query language changes before ID3.

There was a discussion about the relation between the VP draft and the ISO specifications.

This question will be raised in the mailing list.