ISO-OIDF alignment on the mdoc profile of OID4VP over the Browser API

2025-01-17

Ask for ISO from OIDF is to review items in the table in section 3

—

Background: This document was started during the ISO WG10 meeting in Sydney (October 2024) with the objective of clarifying 18013-7 specification requirements for the OpenID4VP specification in order to support Browser APs.

This document: https://docs.google.com/document/d/1AJDDWuRG_b-MOBrAwhBoQV3dhH3LD31WNEQKzOB36SY/edit?tab=t.0

Context and Asks from ISO SC17 WG10

Problem statement: If we use the browser APIs what protocol do we use? The browser API requires the specification of an additional protocol. Ideally, there should be only one protocol.

Previous decisions in ISO SC17 WG10:

1. Browser API to be used as a 3rd option for Part 7.
2. No request encryption.
3. Interim protocol before OpenID4vp v1 for interop testing.

ASK: OIDF to expedite the development of their protocol.

Response and Asks from OIDF DCP WG

1. The first draft of mdoc profile of OID4VP over the Browser API has been merged into HAIP

URL to HAIP: https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0.html

HAIP was restructured:

- Not be limited to SD-JWT VC
- To be a collection of 4 profiles that can be used independently:
    1. Issuance of IETF SD-JWT VC using OpenID4VCI;
    2. Presentation of IETF SD-JWT VC using OpenID4VP;
    3. Presentation of IETF SD-JWT VC using OpenID4VP over W3C Digital Credentials API

4. Presentation of ISO mdocs using OpenID4VP over W3C Digital Credentials API

2. Timelines for 1.0 Final for OID4VP, HAIP and OID4VCI

Third Implementer's Draft of OID4VP was published December 24th: https://openid.net/third-openid4vp-implementers-draft-approved/

Public Review Period for Proposed Second Implementer's Draft of OpenID for Verifiable Credential Issuance Specification has started on Dec 20th 2024: https://openid.net/public-review-period-for-proposed-second-implementers-draft-of-openid-for-verifiable-credential-issuance/

The plan is to publish 1.0 Final before June 2025 for OpenID4VP, OpenID4VCI, and HAIP. And after that keep working on these specifications and publish versions 1.1, 1.2, etc. that are backward compatible with 1.0 Final.

Below is the list of issues that DCP WG would like to tackle before Final 1.0.

- https://github.com/openid/OpenID4VP/milestone/2

Discussion during the mtg seemed to indicate that TS in ISO is equivalent to Implementers draft in OIDF.

3. Summary of how the ISO requirements are being addressed in OIDF DCP WG

In short, each requirement has an issue or a PR (Pull Request) in OIDF DCP WG's Github repository. Majority of items are either done or on track.

Asks to the WG10:

- **Please provide clarifications for the items in red: done during the WG10 Sapporo mtg.**
- **Would like to get alignment on things that are still open (marked orange).**
- **Please confirm that items marked "Done", and "On track" are correctly marked**
    - **ISO WG said they need a bit more time to review this document to confirm what is done and on-track. Agreed to confirm this at the virtual mtg in January.**
        - **Agreed to come back to setting up a small group call after the virtual mtg in January**
    - What is marked "DONE" is stable and is not expected to change
    - What is marked "On track" is where the direction is more or less set, but discussion is on-going - would be good to get input on the direction
    - When "on track" items are updated, or change to "done", OIDF will notify ISO either through email, or uploading the document to the portal
    - Below is the list of issues that DCP WG is tracking as requirements from ISO - please comment if something is missing or is mislabeled. https://github.com/openid/OpenID4VP/issues?q=is%3Aopen+is%3Aissue+label%3AISO%3F

Will 18013-7 continue to define how to do mdocs over OID4VP without Digital Credentials API? Or should it be defined in HAIP and 18013-7 annex B can point to HAIP? This would resolve the fact that 18013-7 ver 1 Annex B points to OID4VP ID-2, which has diverged from the most recent version of OID4VP (ID3)?

Notes from the ISO WG discussion at the Sapporo mtg:

- Updating annex B is not an option.
- Agreed there is a need to fallback for the browser API
- Strong support for mdoc profile over vanilla OID4VP and mdoc profile for OID4VP over Digital Credentials API should sit in the same place, which is HAIP.
- ISO SC17 WG10 open for OIDF to start working on updating mdoc profile over vanilla OID4VP, based on DCP WG's timelines. (In Sydney, ISO discussed updating mdoc over OID4VP (current Annex B) after OID4VP goes final.)

REQUIREMENTS (for any protocol that runs on top of a browser API):

	Requirements	**Status**	**OpenID4vp v.1.0 / HAIP v.1.0**	**Notes**
1	*Must be functionally the same as the existing (i.e. in ISO/IEC 18013-5 and amendment) device request and device response (i.e. nothing less and nothing more*	*"Nothing more" part*	*Since this one is very generic, would like to focus on the requirements below.*	*The intent with the "nothing more" requirement is to prevent a situation where the protocol has many options that do not add value for the "mdoc over browser API" case but have to be implemented in order to comply with the protocol specification.*
2	Device response structure must be included in the response as specified in ISO/IEC 18013-5.	DONE WG10 needs to confirm that this can be closed. ljordaan@aamva.org confirmed	Already supported by the mso_mdoc format definition which is also used by ISO/IEC TS 18013-7:2024: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#name-presentation-response-4 (latest published draft) This is also defined in 18013-7 and 23220-4.	
3.1	Response must be encrypted by the mdoc to a	DONE WG10 needs to	HAIP mandates response encryption using ECDH-ES for JWE. Outcome of DCP WG discussion is to start by using JWE with ECDH-ES	PR that needs to be merged

	key provided by the RP, and all the details required to have interoperability need to be specified. (Already in B.4.3 of ISO/IEC 18013-7)	confirm that this can be closed.	while working in IETF on JWE with HPKE and/or detached JWE. documented here: https://github.com/openid/oid4vc-haip/issues/131#issuecomment-2539528136 Notes from the ISO discussion in Sapporo: "The way Encryption is done in mdoc profile over OID4VP over the browser API does not have to be the same as how it is done in 18013-7 Annex B". Details of how the encryption is done will further be discussed in the DCP WG. ISO SC17 WG10 would like to provide feedback to that - one venue could be virtual WG10 mtg in January.	https://github.com/openid/oid4vc-haip/pull/155/files
3.2	Apple suggestion: HPKE as a single encryption method	DONE WG10 needs to confirm that this can be closed.	DCP WG have agreed to start this work once HPKE support in JWE becomes available and now use ECDH-ES. documented here: https://github.com/openid/oid4vc-haip/issues/131#issuecomment-2539528136 A note that allows HPKE with JARM has been merged in OID4VP: https://github.com/openid/OpenID4VP/pull/315	
4	mdoc authentication must be bound to the origin, e.g. RP URL (If verifier's value in the request is the different from the origin value passed from the platform, response must fail)	DONE WG10 needs to confirm that this can be closed.	Origin is included in Session Transcript	To protect against *certain* phishing attacks on the same device. PRs merged: https://github.com/openid/oid4vc-haip/pull/146, and https://github.com/openid/OpenID4VP/pull/374
5	Response encryption	DONE WG10	Outcome of DCP WG discussion is that this this requirement adds benefit only when origin can be passed in a	

	authentication must be bound to the origin, e.g. RP URL.	needs to confirm that this can be closed.	detached manner during encryption/decryption, but does not add benefit with JWE ECDH-ES since origin is already passed in a detached manner as part of Session Transcript. DCP WG agreed to tackle this once support for HPKE in JWE becomes available, but do not take any action now: https://github.com/openid/OpenID4VP/pull/380#issuecomment-2596203778 Note that apu/apv values can be chosen by the sender (RP) without impacting interoperability, because in the calculation, receiver (wallet) uses apv/apu values it received. So there is no need to define apu/apv value in mdoc profile of OID4VP over the Browser API	
6	There must be an option for the app to authenticate the key received from the RP to be used for response encryption.	DONE	This is done by having an option to sign the Request to authenticate RP's key. Notes from the ISO discussion in Sapporo: Confirmed that RP authentication in the sense of 18013-5/-7 can be mandatory, but not mandatory for everyone	
7	Must be fully specified (i.e. no allowed options that, when exercised in any way, could lead to non-interoperability).	On track	DCP WG interpreting this as "no parameter negotiation, so every valid parameter combination must behave in an interoperable way". The following is an additional issue important to the interoperability: https://github.com/openid/oid4vc-haip/issues/142: agreed to mandate all DCQL features	
8	There can be an option to sign the request.	DONE Confirmed at the ISO mtg	Already defined in OID4VP: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#name-signed-request	

Below is not a part of the original explicit request from WG10, but came up in the discussion with WG10 members.				
9	ISO/IEC 18013-5 amendment covers extra requirements on query language	DONE	A new query language DCQL has been merged in OID4VP and it is mandated in mdoc profile. Adding intent_to_retain as a mechanism specific to mdocs only, reusing the definition from ISO: https://github.com/openid/OpenID4VP/pull/338	
10	**Subrequests (called usecases now)**	DONE WG10 needs to confirm that this can be closed. ljordaan@aamva.org	Credential_sets in new query language DCQL addresses it: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#name-digital-credentials-query-l	ISO/IEC 18013-5 amendment new request structure
~~11~~	~~**Conditional data elements** (required if present)~~ ~~(looks like discussion will happen in Sapporo)~~	~~On Track~~ During Sapporo mtg confirmed that this is not relevant anymore	~~Yes, this is in DCQL in OID4VP: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#section-6.3.1.1-2.3~~ ~~Open question is here on `claim_sets` processing: https://github.com/openid/OpenID4VP/issues/290~~ ~~Some of this depends on Real ID use-case and conditional data elements discussionin ISO.~~	~~ISO/IEC 18013-5 amendment new request structure~~
12	**Alternative data elements** (optional data elements)	DONE WG10 needs to confirm that this can be closed. ljordaan@aamva.org	Claim_sets in https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#section-6.3.1.1-2.3	ISO/IEC 18013-5 amendment new request structure

13	**Preference indication** for alternative data elements	DONE WG10 needs to confirm that this can be closed. ljordaan@aamva.org	Order in the array in the claim_sets in https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#section-6.3.1.1-2.3	
14	**Issuer selection based on issuer keys** (equals any public key of any certificates in the x509 validation chain)	On Track	Agreed on a new DCQL parameter in this issue on filtering by the Issuer. PR is expected to follow: https://github.com/openid/OpenID4VP/issues/322	
15	**0-N Purpose code(s)** (not free text) for each subrequest	DONE Agreed that no need for any immediate action both in DCP WG and ISO WG	Notes from the ISO discussion in Sapporo: No immediate resolution expected from ISO SC17 WG10 nor DCP WG Jfyi in DCP WG this is being discussed in this issue on “define details for the purpose property”: https://github.com/openid/OpenID4VP/issues/289 Strong preference from DCP WG not to have codes. If ISO has a requirement for codes, please provide examples.	ISO/IEC 18013-5 amendment new request structure
16	**Multiple docs in the response per doctype** if verifier indicated support for this.	On track	Being discussed in this issue: https://github.com/openid/OpenID4VP/issues/298 Notes from the ISO discussion in Sapporo: Clarified that this requirement means returning multiple mdocs of "same doctype, same namespace, same data elements, different value"	ISO/IEC 18013-5 amendment new request structure

17	Multi RP authentication	On Track	PR on track to be merged: https://github.com/openid/OpenID4VP/pull/308	
18	Cross device support	DONE	W3C Digital Credentials API can be implemented with cross-device flow.	

ISO WG4/10 member Invitation to participate in OIDF

- May join mailing list for DCP WG at no cost and with no paperwork, but will not be unmoderated without a signed contributed agreement
- May observe a DCP WG call at discretion of cochairs at no cost, with no paperwork. Calendar and zoom link on OIDF website
- May use OIDF test suite at no cost to run implementations against (wallet side and RP side, for different credential types as OID4VC tests come available)
- May make technical contributions at no cost by signing participation agreement as an individual or an entity
- Option to join as a member for spec voting rights at OIDF, to receive discounts on OIDF self certification. Members may also get free or discounted access to OIDF hosted or co-hosted hackahron and interop events (eg CA DMV & OIDF public sector 11/1/24 and private sector events 10/1/24). Membership is $50 for individuals, $250 for no-profits and governments, and $1,000-$20,000 private entities. Sustaining board seats $50,000. Membership is a key pillar of OIDF sustainability.
- https://openid.net/wg/digital-credentials-protocols/

OIDF welcomes WG 4/10 feedback on thé potential formation of a Digital Identity SDO Community Group

- (cochaired by a lead from each of ISO/ IEC WG 4/10, FIDO, W3C, IETF, OIDF).