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

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 turned into a PR in HAIP: https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122

DCP WG made a decision to restructure HAIP (High Assurance Interoperability Profile) to add mdoc profile of OID4VP over Browser API to HAIP. The following is the summary of the reasoning:

1. Cannot put mdoc profile in OID4VP, because this way, nothing can be mandated (response encryption, session transcript structure, etc.), since OID4VP is a framework.
2. Cannot put mdoc profile into a separate document, and keep HAIP as-is because this would significantly slow things down since DCP WG would need to go through the process of adopting a new document, and work on 4 documents (OID4VCI, OID4VP, HAIP and mdoc profile) in the same WG with tight deadlines. Also, with this approach, it becomes unclear where to put parts of the Browser API profile that are common to both mdoc and sd-jwt vc.

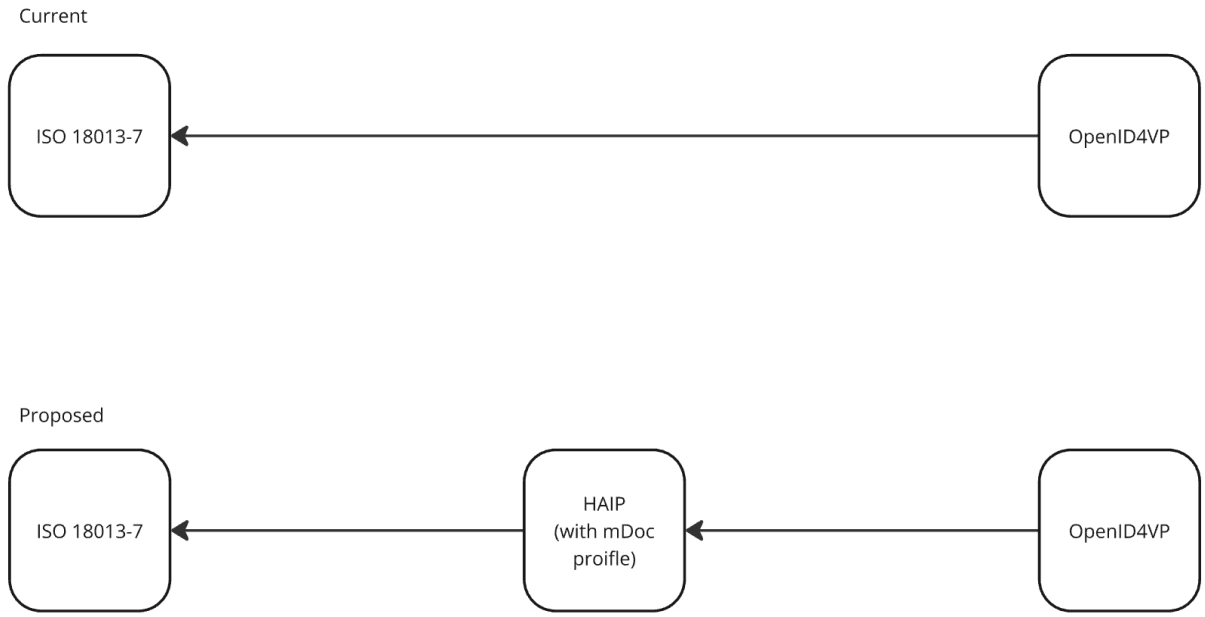
How HAIP is being restructured:

- Not be limited to SD-JWT VC
- To be a collection of 4 profiles that can be used independently (e.g. “Implementations of this specification do not have to implement all of the four flows, but they MUST be compliant to all of

the requirements for a particular flow they chose to implement.” in https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/files#diff-6dce287ad53921b1509d0c72cae65a481a248ccdb7189cd757272b3e62514021R106):

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

For ISO SC17 WG10, this means that ISO 18013-7 document will have to reference HAIP, and not OID4VP:



2. Timelines

The goal is to publish as soon as ready, and as soon as possible.

One data point/requirement from another jurisdiction (European Commission) is for both OID4VP and HAIP to be published as Final specification no later than in June 2025.

Third Implementer’s Draft of OID4VP is expected to be published December 24th.
First Implementer’s Draft of HAIP is expected to follow.

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**
- **Please confirm that items marked "Done", and "On track" are correctly marked**
- **Would like to get alignment on things that are still open (marked orange).**

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. ljord…	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 key provided by the RP, and all the details required to have interoperability need to be specified.	On Track	DCP WG Agreement in Response Encryption in mdoc profile in HAIP: https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/files#diff-6dce287ad53921b1509d0c72cae65a481a248ccdb7189cd757272b3e62514021R231 Needs ISO WG's input. Currently assumes using Response encryption mechanism is as already defined in 18013-7. But sounds like SessionTranscript should be	

	(Already in B.4.3 of ISO/IEC 18013-7)		incorporated into JWE: https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/files#diff-6dce287ad53921b1509d0c72cae65a481a248ccdb7189cd757272b3e62514021R240 ljordaan@aamva.org	
3.2	Apple suggestion: HPKE as a single encryption method	Discussion on on-going in DCP WG	A note that allows HPKE with JARM has been merged in OID4VP: https://github.com/openid/OpenID4VP/pull/315 The rest of the discussion is here: https://github.com/openid/OpenID4VP/issues/310	
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)	On Track	Origin is included in Session Transcript Line 257 in https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/files#diff-6dce287ad53921b1509d0c72cae65a481a248ccdb7189cd757272b3e62514021R257 Need ISO WG's input whether mDocGeneratedNonce is needed and whether Hashing is needed. ljordaan@aamva.org	To protect against *certain* phishing attacks on the same device. Envelope focus
5	Response encryption authentication must be bound to the origin, e.g. RP URL.	On Track	Origin is included in Session Transcript Line 258 in https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/files#diff-6dce287ad53921b1509d0c72cae65a481a248ccdb7189cd757272b3e62514021R258 [Same as above] Needs ISO WG's input. Currently assumes using Response encryption mechanism is as already defined in 18013-7. But sounds like SessionTranscript should be incorporated into JWE: https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/files#diff-6dce287ad53921b1509d0c72cae65a481a248ccdb7189cd757272b3e62514021R240	To protect against certain phishing attacks on the same device WG10 discussion: MH: Data elements focus #4 and #5 bound together by doing both. So both are required.

6	There must be an option for the app to authenticate the key received from the RP to be used for response encryption.	On Track	This is done by having an option to sign the Request to authenticate RP's key is enabled: https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/files#diff-6dce287ad53921b1509d0c72cae65a481a248ccdb7189cd757272b3e62514021R227 That builds up on https://openid.github.io/OpenID4VP/openid-4-verifiable-presentations-wg-draft.html#name-signed-request And https://openid.github.io/OpenID4VP/openid-4-verifiable-presentations-wg-draft.html#section-5.1-4.2.1 Need to confirm with ISO WG if mandating to sign the request is prohibited or not. eIDAS 2.0/EU requirements are to sign the request, so DCP WG needs to know. ISO 18013-5 says: "An mDL may require mdoc reader authentication (see 9.1.4) before releasing data elements not marked as mandatory in Table 5. An mDL shall not require mdoc reader authentication as a precondition for returning any of the mandatory data elements. An mDL may offer functionality to the mDL holder to pre-authorize the return of mandatory data elements selected by the mDL holder to mDL readers using mdoc reader authentication." and ISO 18013-7 says "The mDL data model descriptions and requirements in ISO/IEC 18013-5 shall apply in this document with the following exception: an mDL may require mdoc reader authentication as a precondition for the release of any of the mandatory data elements." so in 18013-7, technically, mdoc reader authentication (eg verifier authentication) can be mandated as a pre-condition to release both mandatory and not mandatory data elements.	Mechanisms to be supported are: ● Key in a certificate. ● A key signed with a key that is authenticated by a certificate.

7	Must be fully specified (i.e. no allowed options that, when exercised in any way, could lead to non-interoperability).	On track	PR that specifies the details is in: https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/	
8	There can be an option to sign the request.	DONE WG10 needs to confirm that this can be closed. ljord…	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: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html#name-digital-credentials-query-l And it is mandated in mdoc profile: https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/files#diff-6dce287ad53921b1509d0c72cae65a481a248ccdb7189cd757272b3e62514021R231 Few open discussions regarding DCQL in DCP WG that might be relevant and ISO WG input is appreciated: - Intent_to_retain: https://github.com/openid/OpenID4VP/issues/321#issuecomment-2491737977 - Value matching: https://github.com/openid/OpenID4VP/issues/307 - Can we use path for mdocs too: https://github.com/openid/OpenID4VP/issues/293	

10	**Subrequests**	DONE WG10 needs to confirm that this can be closed. ljord…	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	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. ljord…	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. ljord…	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	On Track	Being discussed in this issue on filtering by the Issuer: https://github.com/openid/OpenID4VP/issues/322	ISO/IEC 18013-5 amendment new request structure

	in the x509 validation chain)			
15	**0-N Purpose code(s)** (not free text) for each subrequest	Needs clarification	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 an example. ISO WG input required.	ISO/IEC 18013-5 amendment new request structure
16	**Multiple docs in the response per doctype** if verifier indicated support for this.	Needs clarification	Returning multiple mdocs is allowed: https://github.com/openid/oid4vc-haip-sd-jwt-vc/pull/122/files#diff-6dce287ad53921b1509d0c72cae65a481a248ccdb7189cd757272b3e62514021R238-R239 Sounds similar to the issuer here, where a property to the "meta" parameter could be added: https://github.com/openid/OpenID4VP/issues/298 ISO WG discussion required.	ISO/IEC 18013-5 amendment new request structure
17	Multi RP authentication	Needs clarification	Solution discussed in here: https://github.com/openid/OpenID4VP/issues/248 PR is in: https://github.com/openid/OpenID4VP/pull/308 ISO WG discussion required.	
18	Cross device support	DONE	W3C Digital Credentials API by definition supports 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).