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

2025-April-23

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 Digital Credentials APIs what protocol do we use? The Digital Credentials API requires the specification of an additional protocol. Ideally, there should be only one protocol.

Previous decisions in ISO SC17 WG10:

1. Digital Credentials 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 Implementer's draft of HAIP has been published:
https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0-ID1.html

Announcement is here.

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

The plan is to have stable versions (that will be published as Final 1.0) of OpenID4VP, OpenID4VCI, and HAIP before the end of June. 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 and PRs 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.

REQUIREMENTS (for any protocol that runs on top of a Digital Credentials 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 Digital Credentials 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 Confirmed at Jan-2025 ISO mtg	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. (Already in B.4.3 of ISO/IEC 18013-7)	DONE Confirmed at Jan-2025 ISO mtg	HAIP mandates response encryption using ECDH-ES for JWE. Outcome of DCP WG discussion is to start by using JWE with ECDH-ES 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 Digital Credentials API does not have to be the same as how it is done in 18013-7 Annex B".	PR that needs to be merged https://github.com/openid/oid4vc-haip/pull/155/files
3.2	Apple suggestion: HPKE as a single encryption method	DONE Confirmed at Jan-2025 ISO mtg	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 Confirmed at Jan-2025 ISO mtg	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 authentication	DONE Confirmed at	Outcome of DCP WG discussion is that this requirement adds benefit only when origin can be passed in a detached manner during	

	must be bound to the origin, e.g. RP URL.	Jan-2025 ISO mtg.	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 Digital Credentials 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 Confirmed at Jan-2025 ISO mtg	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: all DCQL features are mandatory https://github.com/openid/oid4vc-haip/pull/151	Requirement is meant to say that it must be clear for both RP and Wallet which features are mandatory and which are not.
8	There can be an option to sign the request.	DONE Confirmed at Jan-2025 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 Confirmed at Jan-2025 ISO mtg	A new query language DCQL has been merged in OID4VP and it is mandated in mdoc profile. Added 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 Confirmed at Jan-2025 ISO mtg	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 Confirmed at Jan-2025 ISO mtg	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 Confirmed at Apr-2025 ISO mtg	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 Clarification PR merged: https://github.com/openid/OpenID4VP/pull/450	

14	**Issuer selection based on issuer keys** (equals any public key of any certificates in the x509 validation chain)	DONE Confirmed at Apr-2025 ISO mtg	Agreed on a new DCQL parameter in this issue on filtering by the Issuer. PR merged: https://github.com/openid/OpenID4VP/pull/393 AKI is for ISO use-cases https://openid.github.io/OpenID4VP/openid-4-verifiable-presentations-wg-draft.html#name-authority-key-identifier	
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.	DONE Confirmed at Utrecht hybrid mtg	PR merged: https://github.com/openid/OpenID4VP/pull/398 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" Got feedback multiple allowed mechanism in 18013-5 rev2	ISO/IEC 18013-5 amendment new request structure
17	Multi RP authentication	DONE Confirmed at Apr-2025 ISO mtg	PR merged: https://github.com/openid/OpenID4VP/pull/308	
18	Cross device support	DONE Confirmed at	W3C Digital Credentials API can be implemented with cross-device flow.	

		Jan-2025 ISO mtg		
19	RP has to specify exactly which data elements it needs. Do not permit an option to request all data elements.	DONE Confirmed at Utrecht hybrid mtg	In 18013-5, RP has to explicitly specify which data element it needs. (“collection limitation” would be a keyword to look for) PR merged: https://github.com/openid/OpenID4VP/pull/424	OpenID4VP/issues/304
20	same credential fulfilling multiple credential queries	DONE Confirmed at Apr-2025 ISO mtg (unless Ketan reaches out before Apr-17 EOD)	PR expected to be merged before the next virtual ISO mtg: https://github.com/openid/OpenID4VP/pull/492	

Discussion notes from april 17th 2025 virtual mtg:

- apu/apv discussion:
  - Defining apu/apv does not solve “lazy” verifier problem, because verifier can successfully derive a decryption key using apu/apv values it receives from the wallet, even if apu/apv values are opaque to the verifier
  - How apu/apv is used is protocol specific.
  - Defining apu/apv value and mandating verifier to check those might help with failing early by verifier being able to detect MITM / defence in depth / for non-mdoc credentials
    - KY: don’t think apu/apv can be hash of sessionRranscript since that would be limited to mdocs… origin, nonce are probably better candidates for apu/apv values
  - DCP WG is checking if NIST recommendation to define apu and apv applies to this openid4vp over dc api use-case. If confirmed, might need to define those. https://github.com/openid/OpenID4VP/issues/414
  - **Agreed to continue the discussion DCP WG/issue on adding a mechanism in OpenID4VP how to communicate from the wallet to the verifier which value are used in apu/apv when they are specified and/or for any other**

mechanism that uses detached input for AEAD (such as JOSE-HPKE): https://github.com/openid/OpenID4VP/issues/347
    - KY: we could say in openid4vp that it is up to the profiles to define and in HAIP to define apu/apv to be origin/nonce?
- **This has been discussed in DCP WG on Apr-22nd: https://lists.openid.net/pipermail/openid-specs-digital-credentials-protocols/Week-of-Mon-20250421/000756.html**
    - The following guidance was provided by NIST on that call:
        - NIST SP 800 does not strictly require APU/APV to be conformant (recommended, not required) and if the motivation is mainly compliance to SP 800, then there is no need to worry about it.
        - the language in 800 will be cleaned up and the intent was not to make this a requirement (APU/APV not being null).
        - If the main goal is to protect against a lazy verifier, then including values in the KDF computation can help, but only if those values are generated independently. If APU/APV values are being sent (not detached), then it might not really help with lazy verifiers. If implicit values cannot be used, then there might still be some benefit, but limited and a discussion if that is really needed is fair to have.
        - It is arguably a "hygiene" issue, but there doesn't seem to be a clear benefit (of defining APU/APV values if they are explicit) and that Andrew was confused by the relation to the lazy verifier problem.
    -
- HPKE
    - This is the current WG agreement: https://github.com/openid/oid4vc-haip/issues/131#issuecomment-2539528136
    - Which resulted in this current text in openid4vp: https://openid.github.io/OpenID4VP/openid-4-verifiable-presentations-wg-draft.html#section-8.3-7
    - This issue is open to improve this current text to meet implementation requirements: https://github.com/openid/OpenID4VP/issues/347