The OpenID Foundation (OIDF) is a non-profit international standardization organization of individuals and companies committed to enabling, promoting and protecting OpenID technologies. Formed in June 2007, the Foundation serves as a public trust organization representing the open community of developers, vendors, and users. OIDF assists the community by providing needed infrastructure and help in promoting and supporting expanded adoption of OpenID Connect and its extensions. Today OpenID Foundation standards are mature and widely adopted:
- OpenID Connect is used by billions of users to access services from over a 100 million consumer and enterprise applications.
- Financial-Grade API standards have been adopted by the governments of the UK, Australia and Brazil to support economy-wide Open Banking implementations.

We would like to offer the following comments on two questions posed by DHS:

**Question 11.b. Offline and Online Data Transfer Modes.** “Provide comments on the security protocols that would be required to mitigate security and privacy risks presented by both offline and online data transfer modes.”

The OpenID Foundation applauds the choice of ISO/IEC 18013-5 to use OpenID Connect as one of the optional online data transfer modes.

OpenID Connect is a modern identity protocol built on OAuth 2.0 that enables third-party authentication to applications in a standard way and has been deployed and used by billions of people since its
publication in 2014. OpenID Connect was developed within the OpenID Foundation by over 300 members encompassing 36 countries working together using an open process.

The OpenID Foundation acknowledges that its members have contributed to ISO/IEC 18013-5 in defining how OpenID Connect can be used to retrieve data between the mdoc reader and the issuing authority in a secure and privacy-preserving manner.

The OpenID Foundation is confident that the model adopted in ISO/IEC 18013-5 addresses currently known security and privacy risks when implemented in compliance to the specification. The model is designed to prevent known attacks, such as the authorization code injection attack, redirect URI validation attack, and cross-site scripting by avoiding the implicit flow, redirects, log files and headers, just to name a few restrictions taken.

Mitigating solutions to the known attacks have been documented by industry experts as a Security Best Current Practice specification for OAuth 2.0, a protocol supporting OpenID Connect, to cover new threats based on the practical experiences. The most recent document can be found here: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-security-topics-18.

When developing browser-based applications that use OAuth 2.0, security considerations and best practices have also been detailed in a specification, found here: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-browser-based-apps-08.

**Question 4.(e). Industry Standard ISO/IEC 18013-5: Communication Interfaces Between mDL Device & Federal Agency & Federal Agency and DMV, “Identify what if any alternative standards...should be considered.”**

Currently the standard includes a few well known communication protocols between the user’s device and the relying party: near-field communication (NFC), Bluetooth, and wifi-aware. OpenID Connect Self-issued OpenID Provider is one of the optional online data transfer modes for both “attended” and “unattended” use-cases.

Self-Issued OpenID Provider model enables End-Users to use OpenID Providers (OPs) that they control, and it has been originally defined in OpenID Connect Core 1.0 Section 7. When OpenID Connect is used, the issuing authority sends data directly to the mdoc reader upon receiving the access token from the mdoc (call home). A Self-Issued OpenID Provider can meet additional privacy-preserving requirements in the upcoming enhancements to ISO/IEC 18013-5 (ISO 18013-7 and 23220 series) to enable online data transfer directly between the mdoc and the mdoc reader without the mdoc reader contacting the issuing authority.

The Self-Issued OpenID Provider work has been contributed to 18013-7 and 23220 series in ISO/IEC SC17 JTC1 WG 4 and WG10 Please refer to Annex A for the full adopted OIDF “Self-Issued OpenID Provider” proposal to ISO.

There is additional work to be completed before this work could be adopted by DHS, but the active participation of DHS/ NIST and other federal entities in OIDF AB/Connect Working Group and ISO18013-5 & 23220 are welcome to help expedite the evaluation and development of this work, to inform its application for federal use cases.
It is worth noting that mDL use-case extends Self-Issued OpenID Provider model, by introducing a requirement for verifier and OpenID Provider to be on the separate devices, such as mdoc reader and mdoc. AB/Connect Working Group in OpenID Foundation is carefully considering security implications of such a model. Client Initiated Backchannel Authentication (CIBA) flow is also being considered as one of the potential alternatives to make such flow more secure. Outcomes of these considerations will be contributed to ISO/IEC JTC1 SC17 WG4, when finalized.

Finally, the OpenID Foundation would like to note the potential interoperability of between OpenID Connect and W3C Verifiable Credentials, an emerging standard that is perceived to be a foundation capability to enable decentralized identity services at scale.

We are currently working on a specification that enable W3C Verifiable Presentations to be transported using any OpenID Connect flow. In particular Self Issued OpenID Provider model can be used to release a mDL expressed as a W3C Verifiable Presentation, which would allow the mDoc reader to cryptographically verify if the presenter of the claim is a legitimate holder of the claim. This is particularly important in scenarios where 18013-5 is used for identity proofing, device binding, or holder binding capability. This model could also enable extending mobile ID use cases to allow exchange of additional data beyond that on the mDL.

For Verifiable Credentials approach, there is more work to be done by the ISO community to flesh it out both in terms of formalizing within the standards, and assessing and establishing the operational processes required to ensure it meets appropriate privacy-preserving, secure and scale requirements. It is worth noting this effort are complementary and aligned with active and ongoing efforts to scale adoption for economy-wide “unattended” acceptance.

Thank you for your consideration.

Regards,

Nat Sakimura
OpenID Foundation Chairman
On behalf of the AB/Connect Working Group of the OpenID Foundation

Annex A
OIDC SIOP (Self-Issued OP) proposal

Contributors: Anthony Nadalin, Kenichi Nakamura, Kristina Yasuda

Introduction

This contribution is aimed to introduce the OIDC SIOP (self-issuing OIDC provider) model to ISO/IEC 23220 series and ISO/IEC 18013 Part 5.

With a physical driving licence, the issuing authority has no knowledge of who the user is showing their driving licence to. However, the OIDC protocol specified in ISO/IEC 18013-5 requires that the issuing authority (OpenID provider) must know about and communicate with the mDL reader. This may violate the user’s privacy.

In this OIDC SIOP model, the mobile device runs an OIDC SIOP service along with the mdoc application. When a user wishes to send their identity (and attribute) information to an mdoc reader, they select OIDC SIOP for authentication rather than the issuing authority infrastructure. When an mdoc reader sends an information request to the mdoc holder’s OIDC SIOP on the mobile device, the OIDC SIOP requests the mdoc application to present the mdoc. The mdoc application returns an ID Token to the mdoc holder’s OIDC SIOP. The mdoc holder’s OISC SIOP returns it to the mdoc reader.

W3C Verifiable Credential data model (i.e., Verifiable Presentation) is also applicable to ID Token. As a result, a user can present identity (and attribute) information to the mdoc reader without sharing any information with the issuing authority.

We wish to contribute,

- To ISO/IEC 23220-1 proposing an additional architecture.
- To ISO/IEC TS 23220-4, proposing a generic OIDC SIOP framework.
- To ISO/IEC 18013-5, proposing OIDC SIOP amendment referencing to ISO/IEC 23220-4 OIDC SIOP framework.

Editor’s NOTE: Amendment to ISO/IEC 18013-5 or ISO/IEC TS 18013-7?
Editor’s NOTE: Open items--> Capability exchange

- Disambiguation data (two possibilities)
  - Add the SIOP options to RetrievalOptions with the following CDDL structure:

```cddl
RetrievalOptions = WifiOptions / BleOptions / NfcOptions / ServerUrlOptions / OidcSiopOptions

OidcSiopOptions = {
    0: tstr ; URL of the verifier server
    1: boolean : OIDC SIOP Client support
}
```
- Add the SIOP capability to ServerUrlOptions with the following CDDL structure

```cddl
ServerUrlOptions = {
    0: tstr ; URL of the verifier server
    ?1: unit ; 1 OIDC SIOP Client support
        2 RESTAPI Verifiable presentation mapping
}
```

**Normative references**

RFC 8252, OAuth 2.0 for Native Apps

OpenID foundation, OpenID Connect Core 1.0 incorporating errata set 1

[https://openid.net/specs/openid-connect-core-1_0.html](https://openid.net/specs/openid-connect-core-1_0.html)

OpenID foundation, OpenID Connect Discovery 1.0 incorporating errata set 1,

[https://openid.net/specs/openid-connect-discovery-1_0.html](https://openid.net/specs/openid-connect-discovery-1_0.html)

**Proposal to ISO/IEC 23220-1**

*P11, 3.31,*

Add the following definition after 3.31:

3.32 remote user storage

remote storage service that is used by a user with access authorization by the user being required if someone wishes to retrieve data from this storage

*P29, 10.2,*

Add the following paragraphs and figure after Figure 17 and replace the last two paragraphs with:

A user may use a Remote User Storage Service instead of Identity and Attribute Provider Service as described in Figure 18. In this case, a user transmits user attributes via mobile eID-App and also allows a Service Provider to access to the user's Remote User Storage. Then a Service Provider may access the user's Remote User Storage and retrieve additional user attributes (see interface PR-7 in Figure 18). The interface PR-4 (see Figure 17) may also be supported in this architecture. This prevents the Identity and Attribute Provider Service from knowing the access log for the user's attributes.
This system architecture includes the Verification Application, the Identity or Attribute Provider and mobile eID-App with interfaces PR-1, PR-3, PR-4, PR-5, PR-6 and PR-7 in Figure 16 and Figure 17.

The verification and revocation infrastructure service of this system architecture may be operated by a separate service or by one single service and includes relation PR-3 in Figure 16 and Figure 17.

Proposal to ISO/IEC TS 23220-4

7.1.3.4 OIDC SIOP (Self-Issued OpenID Provider)

7.1.3.4.1 OIDC SIOP model

OIDC SIOP is an extension of OpenID Connect (see 7.2.1) to allow a mdoc holder to use OpenID Providers (OPs) that they control and present mdoc data directly to mdoc reader as a device retrieval method and it prevents the issuing authority from knowing usage information of mdoc data via communication with the mdoc reader. OIDC SIOP is specified in OpenID foundation, OpenID Connect Core 1.0 incorporating errata set 1, Section 7.

Figure 1 describes the OIDC SIOP system architecture.
This document specifies interface between OIDC SIOP and OIDC Client that is used for data retrieval. Additionally, the use of OIDC UserInfo endpoint is also specified. The discovery of the location of the OIDC UserInfo endpoint is out of scope of this document.

The interface between the holder and OIDC SIOP is required for user authentication for the mdoc data retrieval service and the requirements for this interface are out of scope of this standard. The interface between the Issuing Authority and OIDC SIOP is also out of scope. OIDC SIOP is applicable to remote identification system architecture (see ISO/IEC 23220-1, Clause 10). OIDC SIOP is supported by mobile eID-app and OIDC Client is supported by the Service Provider (see ISO/IEC 23220-1, Clause 10, Figure 14). In this document, the OIDC SIOP may support the UserInfo endpoint and provides additional information, which includes claims not included in the ID Token.

Editor's note We need to propose to add "remote user storage" entity in ISO/IEC 23220-1 for supporting the UserInfo endpoint.

The protocol between OIDC SIOP and OIDC Relying Party consists of the following four steps:

---
- SIOP discovery (see 7.1.3.4.2)
- SIOP registration (see 7.1.3.4.3)
- Authorization Request and ID Token retrieval (see 7.1.3.4.4)
- ID Token validation (see 7.1.3.4.5)
---
7.1.3.4.2 SIOP discovery

For SIOP discovery, OpenID connect dynamic discovery is not applicable and a static configuration may be used. If static configuration is not used, the value of the configuration parameters should be negotiated between OIDC SIOP and OIDC Client in advance.


The description of the URL that is used to invoke SIOP may be custom URL schema or universal URLs. If SIOP supports multiple mdocs, then OIDC SIOP and OIDC Client shall negotiate a mechanism to invoke a particular mdoc in advance.

The static configuration shall support URL of UserInfo endpoint, if OIDC SIOP support UserInfo endpoint.

7.1.3.4.3 SIOP registration

The OIDC registration process is required for SIOP. OIDC Client may use the "registration" element in the Authorization Request, as specified in OpenID Connect Core 1.0 incorporating errata set 1, 7.2.1.

7.1.3.4.4 Authorization request and ID Token retrieval

OIDC Client sends the Authorization Request to the Authorization endpoint of SIOP, as specified in OpenID Connect Core 1.0 incorporating errata set 1, 7.3.

If OIDC Client indicates the intent to store the data at the data element level, then the Boolean field "intent to store" shall be mapped to each claim.

EXAMPLE

```json
{
    "claims": {
        "id_token": {
            "verified_claims": {
                "claims": {
                    "claims": {
```
"given_name": {  
  "intent_to_store": true
},

"family_name": {  
  "intent_to_store": true
},

"birthdate": null,

"nationality": null,

"address": null

}

SIOP sends the Authorization Response to the OIDC Client as specified in OpenID Connect Core 1.0 incorporating errata set 1, 7.4. An ID Token shall be returned if OIDC Client sends a SIOP Authorization message.

The "verified_claims" container element used in the example above is taken from OpenID Connect for Identity Assurance 1.0 specification (ekyc-ida) in OpenID Foundation. The usage of "verified_claims" container element allows to include information how the identity of a natural person has been verified in compliance with a certain law.

It should be noted that the value of iss (issuer) claim in SIOP response is https://self-issued.me and it does not indicate the issuer of the mdoc.

The following example shows the claims of the JWT:

{
  "iss": "https://self-issued.me",
  "iat": 1611543618,
  "exp": 1611543918,
  "aud": "https://utopiadot.gov/resources",
  "sub": "1",
  "doctype": "org.iso.18013.5.1.mDL",
  "given_name": "(CBOR encoded given name)"
"family_name": "(CBOR encoded family name)",
"birth_date": "1971-09-01",
"MSO": "(CBOR encoded MSO blob)"
}

The device authentication key as specified in ISO/IEC 18013-5, 9.1.3.4 shall be used for signing the ID Token. A JWK Thumbprint shall be used as the subject identifier for SIOP.

The OIDC SIOP may send an Access token in addition to an ID Token.

NOTE The current OpenID Connect specification does not specify the use of an Access token by SIOP.

If not all the requested claims are included in the ID Token, such claims can be provided via a UserInfo endpoint hosted by the user. An access token can be used to access the UserInfo endpoint. The access token enables retrieving claims from the UserInfo endpoint.

7.1.3.4.5 ID Token validation
The mdoc reader validates the ID Token as specified in OpenID Connect Core 1.0 incorporating errata set 1, 7.5.

7.1.3.4.6 Access to UserInfo Endpoint
OIDC Client may send UserInfo request to UserInfo endpoint. The use of UserInfo endpoint is specified in OpenID Connect Core 1.0 incorporating errata set 1, 5.3.