Engagement letter with OIDF

From: SAGSTETTER Norbert

To: OIDF Executive Director Gail Hodges, gail@oidf.org

Subject: OIDF engagement in the update and creation of Technical Specifications (TS) for the implementation the European Digital Identity Wallet (EUDI) ecosystem

The European Commission (EC) has initiated a structured process to build a sustainable standards and technical specifications infrastructure, that will enable and facilitate the implementation of the EUDI Wallet ecosystem, as defined in Regulation (EU) 2024/1183[1] (eIDAS).

Parallel to the development of the Regulation, the EC, in collaboration with experts from EU Member States, has prepared an Architectural Reference Framework (ARF), which is available at https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/latest/arf/. Apart from describing the envisaged technical and procedural implementation of the EUDI Wallet ecosystem, the ARF also contains high-level technical requirements (HLTR) for the components of this ecosystem, their interactions and interfaces.

In, this context, the EC prepared a list of standards and technical specifications to be referenced in Implementing Legislation which is under preparation. The EC also described the status of these standards and TS, and updates that are needed to ensure that they fulfil the requirements of the EUDI Wallet ecosystem. Finally, the EC analysed the standardisation gap, that is - for which HLTR in the ARF, there are currently no standards or TS available. Based on this analysis, the EC created a roadmap to fill the gap and ensure that the necessary standards and TS become available with respect to the timeframes set in the Regulation.

The EC has already initiated an engagement process with the recognized SDOs according to Regulation 1025/2012[2] and would like to initiate such a process also with relevant non-recognised SDOs including OIDF. The purpose of this engagement process would be to align on the TS gaps and to consider possible collaboration on how to fill them.

[1] https://eur-lex.europa.eu/eli/reg/2024/1183/oj

[2] https://eur-lex.europa.eu/eli/reg/2012/1025/oj

In Annex A you will find a high-level description of the planned EC standardization strategy regarding the EUDI Wallet ecosystem and the current state of play of its implementation.

In Annex B you will find an initial analysis of existing and in-progress TS that are produced, published or in-progress, by your organization, as well as identified gaps. These identified gaps are just an initial starting point to ensure we're on the same page for the discussions we want to have with you. They are not exhaustive at this stage.

We are looking forward to coordinating an initial meeting so that wo could start this engagement process with you. We will be in contact with you to arrange the meeting as soon as possible.

With best regards,

SAGSTETTER Norbert

CC:

Joseph Heenan, Digital Credentials Protocols WG chair
Torsten Lodderstedt, Digital Credentials Protocols WG chair
Kristina Yasuda, Digital Credentials Protocols WG chair

Annexes

Annex A - Highlights of the EC standardization strategy

1. Background:
    a. The EC has prepared a thorough **Standardization strategy** (hereinafter called also - "strategy") related to the EUDI Wallet ecosystem implementation as derived from the Regulation (EU) 2024/1183[1] (eIDAS/ eIDAS Regulation). This strategy is a comprehensive plan designed to establish, promote and maintain standards and TS within the digital identity domain. This strategy focuses on creating and implementing standards and TS that ensure the EUDI Wallet ecosystem is consistent, secure, GDPR compliant, interoperable and user-friendly across all EU Member States. It will align with existing relevant standards and TS to ensure coherence and compliance across the board as for the implementation of the Regulation.
    b. An important point is that Technical Specifications produced by non-recognized SDOs can become eligible for reference in the IAs through the European Multi-Stakeholder Platform on ICT Standardisation (MSP), or by any other accepted legal process. As such, we will put an emphasis on the current status of the TS produced by your organisation, regarding the MSP process, as will be discussed in Annex B.
    c. The key components of the strategy are:
        i. Assessment: Analyse current practices against the latest EUDIW Architectural Reference Framework (ARF)[3], to identify gaps in HLTR for implementing the eIDAS Regulation.
        ii. Planning: Identify the nature of the gaps and plan a course of action for closing them. This involves determining whether gaps can be filled by existing TS, or do they require the development of new TS, or there should be in place interim TS.
        iii. Support for Implementing Acts: Assist in the preparation of the Implementing Acts by providing comprehensive analysis, gap identification and recommendations for referencing standards and TS.
        iv. Public Procurements: Facilitate the use of standardized solutions in public procurements by referencing approved standards and TS.

[3] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework

d. An initial gap analysis has been carried out. The results are summarized in a few Gap Analysis Report documents - one for each Implementing Acts batch. These documents touch upon the different topics that are included in the ARF in respect of the IAs and point out the gaps, as far as can be foreseen at this stage, and as a basis for discussion and collaboration – specifically with non-recognized SDO's which are the focus of the current effort, as described in more detail below.

2. Purpose of this phase:
   a. The engagement with non-Recognized SDOs is needed so that both the EC and the non-Recognized SDO's will align on a common gap analysis, and the work needed to close the gap with each non-SDO.
   b. More precisely, there is a need to agree on the following:
      i. Confirm the common understanding of the technical gaps that were found.
      ii. Agree on the support of existing standards or technical specifications regarding the required functionalities derived from the technical requirements, sorted into the following categories: (1) fully supported; (2) partially supported; or – (3) not supported at all.
      iii. Map the requirements into: (1) Existing standards and TS published; (2) existing standards and TS in draft stage or under development by SDOs; (3) existing TS produced by non-recognized SDOs; or – (4) needs not covered by any available standards or TS.
   c. This letter includes an initial gap analysis to commence the discussions with non-recognized SDO's. Following this letter, meetings with each non-recognized SDO will be organized, to achieve the following:
      i. Receive feedback on the initial gap analysis, such as: Is it complete? Are there any missing gaps? Are there currently any activities taken to work on the TS, and if so – in which stage are they and what is the predicted time for completing the draft stages and publishing an approved version of the TS? This information is essential for the projection of timelines and expected elapse time for reference in the IAs.
      ii. Collaboration to influence the development or enhancement of TS by contributing to working groups, providing technical input, and participating in the drafting process.
      iii. Identify major functionalities that require new or updated TS.
      iv. Monitoring the progress to ensure that the necessary updates to, or the development of new TS, are addressed in a timely manner.

v. Coordinate and mutually agree upon the plans for developing TS by non-recognized SDOs, respecting of course the autonomous nature of the SDOs, while facilitating the ability to refer to these TS in the Implementing Acts based on the MSP process as default, or another acceptable process if needed.

vi. Ensure that the developed TS meet the EUDIW technical requirements and are eligible for reference in the Implementing Acts.

Annex B - Initial gap analysis for OIDF

1. Standards and specifications referenced in the ARF
    a. Overview

    This section mentions TS that are directly referenced in the ARF. Note that these TS may reference other TS, which in turn reference yet more TS. These referred-to TS may be indispensable for implementing the EUDI Wallet ecosystem. However, none of these referred-to TS are listed in this document, as it concerns finished and publicly available TS and can be found by consulting the TS listed in this chapter.

    b. Published TS

    The rational to include already existing and published TS is the following:

    - To ensure no TS that seems relevant from your point of view, was not omitted.
    - To gather information whether there is an ongoing work to produce a new version of a specific TS, and if so – what is the timeline?

    Note: Where no version number and date are mentioned, the latest published version applies.

    Question: Among TS that are currently referenced by the ARF, the TS published by OIDF are in "draft" stage, and not as "Final Specifications". Please confirm this status.

2. Draft standards and specifications
    For this category, we would like to receive your feedback on the following questions regarding the TS mentioned in the following table:
    - Please confirm what is the current stage of the TS in the OIDF approval process.
    - What is the expected time for completion and publication of the "Final Specifications"?
    - Are you aware of any intention or initiative to pass these an MSP process?

TS	TS name and details	Status	Notes
OpenID4VP	OpenID for Verifiable Presentations - draft 21 O. Terbu et al, 9 August 2024	**IA not-ready** MSP-Unknown (Draft)	
OpenID4VCI	OpenID for Verifiable Credential Issuance - draft 14 T. Lodderstedt et al, 21 August 2024	**IA not-ready** MSP-Unknown (Draft)	
HAIP	OpenID4VC High-Assurance Interoperability Profile with SD-JWT VC – draft 00, 9 January 2024	**IA not-ready** MSP-Unknown (Draft)	This document defines a profile of OpenID for Verifiable Credentials in combination with the credential format SD-JWT VC. The aim is to select features and to define a set of requirements for the existing specifications to enable interoperability among Issuers, Wallets and Verifiers of Credentials where a high level of security and privacy is required. The profiled specifications include OpenID4VCI, OpenID4VP, and SD-JWT VC.

3. <u>Possible Gaps found in referenced standards and specifications that need to be analysed and finalized</u>
   a. For this category, we would like to receive your feedback if the gap is described correctly - as far as you understand the requirements of the Regulation and the ARF, and what are the expected dates for finalizing the TS.
   b. Specifically, we would kindly ask you to clarify the agreement between OIDF and ISO/IEC related to the publication of OIDF TS, and about division of work between them, regarding specifically: ISO/IEC 18013 parts 5 and 7, ISO/IEC 23220 part 4 - and OpenID4VP; and ISO/IEC 23220 part 3 and OpenID4VCI.
   c. <u>OpenID4VP</u>

The following gaps have been identified for OpenID4VP. Please relate to them as in point a) above

#	Description	SDO	Reference to HLR in the ARF
1.	The OpenID4VP document needs to be finalized, approved, and published.	OIDF	OIA_03

#	Description	SDO	Reference to HLR in the ARF
2.	It should be verified whether OpenID4VP (via the Presentation Exchange specification referenced therein) allows a Relying Party to group the attributes they request based on the use case, service, or purpose. If this is not the case, a method for doing so needs to be specified. Comment: The idea of grouping the attributes in the request means that the RP can indicate a goal or purpose per group, and the user can decide to release or not release the attributes per group. This prevents situations where a user refuse consent for one attribute and releases others, while the RP needs all of them to proceed. That would be bad for privacy or user experience. In fact, partly as a result of this requirement, ISO is going to implement this in Amd 1 of 18013-5.	OIDF	RBA_11[4]
3.	Since **OpenID4VP** offers many options, a **profile** is needed to ensure interoperability between all Wallet Instances and Relying Party Instances in the EUDI Wallet ecosystem. In particular., OpenID4VP may be used to request and present both ISO-compliant and SD-JWT VC-compliant attestations. A question, therefore, is whether to allow the transport of ISO-compliant attestations (mdocs) using OpenID4VP, or wants to simplify the situation by requiring that ISO-compliant attestation shall be requested and presented only using the protocol defined in ISO/IEC 18013-7 Annex A: Further work that seems to be done on profiling OpenID4VP: a. For requesting and presenting ISO-compliant attestations, see ISO/IEC 18013-7, section **Error! Reference source not found.**. b. For requesting and presenting SD-JWT VC-compliant attestations, see the HAIP, section d. Note: The basic and generic standards and profiles will be addresses by ISO/IEC for ISO/IEC 18013-7, and by OIDF for HAIP. The work by ETSI is supposed to relate to both generic standards, while defining an EUDIW-specific profile. A preferred approach might be to use the Credential API.	TBD	
4.	A question to be clarified is the relationship between OpenID4VP, ISO/IEC 18013-7 and the W3C browser API. W3C has founded a Federation Identity Working Group that will lead this work. It is understood that the standard will be reflected in an ISO/IEC standard, but this should be verified with W3C. Note that there is a larger discussion where to define how to use OpenID4VP digital credentials API with mso_mdoc: OpenID4VP or ISO. ISO seems to be preferring that to be done in OpenID4VP, but there is no conclusion yet; This will be discussed with both ISO and OIDF.	TBD	

[4] Note this identifier is an error in ARF 1.4.0, it should read RPA_11.

#	Description	SDO	Reference to HLR in the ARF
5.	OpenID4VP must specify two mechanisms allowing revocation of attestations: Attestation Status List and Attestation Revocation List, as defined in Annex 1 of the ARF. This is already proposed for Amendment 1 of ISO/IEC 18013-5. Notes: • The Attestation Status List mechanism is specified in the Token Status List draft RFC, https://datatracker.ietf.org/doc/draft-ietf-oauth-status-list/ . • A proposal for an Attestation Revocation List can be found on GitHub, https://c2bo.github.io/draft-bormann-identifier-list/draft-bormann-identifier-list.html • The High-Assurance Interoperability Profile states that revocation is in scope, but it doesn't contain any requirements, although it references an older version of the Token Status List draft RFC.	OIDF	VCR_09
6.	OpenID4VP must enable a Wallet Instance to transfer a proof of association to a Relying Party, in case multiple attestations are presented in the same response.	OIDF	ACP_09

d. High-Assurance Interoperability Profile (HAIP)

The following gaps have been identified for the HAIP. Please relate to them as in point a) above:

#	Description	Proposed SDO	Reference to HLR
7.	The HAIP document needs to be finalized, approved, and published.	OIDF	
8.	The HAIP includes a section profiling OpenID4VP. This profile is generic and hence also applies when OpenID4VP is used to request and present SD-JWT VC-compliant attestations, in contrast to the profile in ISO/IEC 18013-7. However, the **HAIP profile** for OpenID4VP contains far fewer details compared to the profile defined in ISO/IEC 18013-7, which raises questions on its completeness. OpenID Foundation should be asked to reflect on this and to create a profile that specifies all relevant details and is complete enough to guarantee interoperability. Topics include at least • Defining cryptographic cipher suite(s), i.e., cryptographic algorithms mandatory to be supported by EUDI Wallet Instances and Relying Party Instances. • Supporting Relying Party authentication in compliance with relevant requirements in ARF Appendix 2 and the Common Access CA Certificate Policy (section **Error! Reference source not found.**).	OIDF	RPA_01 RPA_02

e. OpenID4VCI

The following gaps have been identified for OpenID4VCI. Please relate to them as in point a) above:

#	Description	Proposed SDO	Reference to HLR
9.	The OpenID4VCI document needs to be finalized, approved, and published.	OIDF	ISSU_01
10.	A few details must be added or adapted to ensure the protocol specified in OpenID4VCI is fully fit for the purpose of attestation issuance within the EUDI Wallet ecosystem, especially to allow the use of key association as defined in ARF Annex 2 Topic 9. More details can be found in section 7.3 of "Epic 09 - Wallet Trust Evidence", v1.0, NiScy, 2024-03-05.	OIDF	WTE_23 WTE_25 WTE_26 WTE_27
11.	The OpenID4VCI protocol must allow the Attestation Provider to send an embedded disclosure policy for the attestation to the Wallet Instance, where the policy is expressed in accordance with section **Error! Reference source not found.**. Note: It may be that this will not necessarily require a protocol change in VCI, as either the Provider includes the policy in the issued attestation or issues policy as an attestation. To be discussed with OIDF.	OIDF	EDP_08