Adding support for the Aries Framework JavaScript interoperable with the EU ecosystem

Making Aries Framework JavaScript a global framework by making it compliant and interoperable with the standards defined in the European Digital Identity Architecture and Reference Framework (ARF).

Version	Date	Changes
0.1	24-07-2023	Initial proposal with initiatives
0.2	01-08-2023	Added costs, timeline and detailed work items for each of the initiatives
0.3	18-08-2023	Increased the scope of initiative 2 & 4, added start date of Sept. first.

This is a working document, feel free to comment. Animo Solutions B.V. - Contact karim@animo.id for information or participation.

Contents

Introduction
Initiative 1: Mobile Driver's License (ISO/IEC 18013-5) Module - € 29.400
    Outcome
    Item breakdown
Initiative 2: OpenID for Verifiable Credential Support - € 21.900
    Outcome
    Item breakdown
Initiative 3: Hardware Security Module Support for Aries Askar - € 25.650
    Outcome
    Item breakdown
Initiative 4: SD-JWT Module - € 21.750
    Outcome
    Item breakdown
Process Timeline

Introduction

Recently, the EU has been taking big steps toward the regulation and governance of digital identity solutions. This has been causing big waves globally in terms of what standards are gaining recognition. The Architecture Reference Framework (ARF) describes the current understanding of how Digital Identity will function in Europe. It describes the standards, architecture, and flows that the EU digital identity ecosystem needs to support. To build identity solutions that are interoperable and compliant with this ecosystem, new libraries and tools will have to be developed and existing ones adjusted. In this proposal,, we'll explore doing exactly that for Aries Framework JavaScript.

Animo has been contributing to the Hyperledger open-source ecosystem for the past three years, adding significant features and updates to Aries Framework JavaScript, Aries Cloud Agent Python, and other Aries family projects. Especially Aries Framework JavaScript has been a priority of ours. Because of it's modularity and accessibility (due to being a TypeScript framework), we view Aries Framework JavaScript as the easiest way to build solutions that use verifiable credentials. It is especially suited for mobile development but has been gaining momentum for server-side development as well. The recent 0.4.0 release has marked the framework's steps to adopt broader standards and increase interoperability.

Now, we're taking the next logical step by making Aries Framework JavaScript compliant with EU digital identity legislation (current overview of the status). Previously Animo Solutions has executed a similar project by making Aries Framework JavaScript ledger independent. This project was a great success with 8 sponsors and 3 collaborators stepping up. The results of the AnonCreds project can now be used by any developer, organization or government. This ARF project will follow a similar path. The goal is to identify the work that needs to be done, collaborate with partners and sponsors to fund the work, and then implement the work in a coordinated and timely effort. This document is a summary of that first task.

We are actively looking for people that want to contribute to this effort in terms of funding. If you're interested in contributing, please reach out to karim@animo.id. An overview of the expected work packages, costs, and timeline is described below.

The project will start September first and be finalized .....*	
Initiative 1: Mobile Drivers License (ISO/IEC 18013-5) Module	€ 52.500
Initiative 2: OpenID for Verifiable Credential Support	€ 21.900
Initiative 3: Hardware Security Module Support for Aries Askar	€ 29.205
Initiative 4: SD-JWT Module	€ 21.750
Total	€ 116.700
*Start and end date will be dependent on funding progress and will be added to this document later on.	

Initiative 1: Mobile Driver's License (ISO/IEC 18013-5) Module - € 29.400

ISO/IEC 18013-5 is a standard that defines how to share driving license information on mobile devices. Although the specification focuses on driving licenses, the ISO/IEC 18013 group also defines the generic mDoc format. The Architecture Reference Framework (ARF) has adopted this standard to facilitate proximity verification flows.

This module will be built on top of an open-source library developed by Sphereon, to which we will also contribute. The development of this module also requires refactoring the framework's credential and proof format-related logic.

Outcome

A pluggable module for Aries Framework JavaScript that enables storage and verification of mDoc credentials.

Item breakdown

1. Refactoring of format services and moving them out of AFJ's core package
2. Extending AFJ's storage to mDOC (or mDL) Credentials
3. Generalize the existing BLE DIDComm transport to transport mDOC Credentials
4. Integrating with Sphereon's mDoc library

Initiative 2: OpenID for Verifiable Credential Support - € 21.900

OpenID for Verifiable Credentials (OpenID4VC) is a set of specifications for credential issuance and verification on top of OAuth. This 'bundle' currently consists of three specifications:

- OpenID for Verifiable Credential Issuance (OID4VCI)
- OpenID for Verifiable Presentations (OID4VP)
- Self-Issued OpenID Provider v2 (SIOPv2)

In the context of the ARF, the OpenID4VC specification family is used for the issuance and verification of credentials in remote contexts.

Support for OpenID for Verifiable Credential Issuance has already partly been added to AFJ, allowing the holder to receive credentials using the OpenID protocol. However, there needs to be more support for the issuer role as well as verification as a whole.

Outcome

A set of modules allowing for the issuance and verification of verifiable credentials using the OpenID standards.

Item breakdown

1. Implement issuer-side support for OpenID for Verifiable Credential Issuance (using Sphereon's `@sphereon/oid4vci-issuer` library)
2. Add support for OpenID for Verifiable Presentations (using Sphereon's `@sphereon/did-auth-siop` library)
3. Add support for Self-Issued OpenID Provider(using Sphereon's `@sphereon/did-auth-siop` library)

Initiative 3: Hardware Security Module Support for Aries Askar - € 25.650

A Hardware Security Module (HSM) is a dedicated physical computing device that safeguards and manages digital keys and aids in the protection of cryptographic keys. It is engineered to be tamper-resistant to both physical and digital attacks. HSMs are used in scenarios where it's necessary to provide a high level of security and avoid any potential for loss, theft, or compromise of sensitive cryptographic information.

To comply with ARF requirements, configuration type 1 credentials must be backed by an HSM. AFJ can utilize HSMs by adding it to Aries Askar.

Outcome

The result of this work will be an updated version of Aries Askar that is able to integrate with the iOS and Android HSM APIs, as well as an updated AFJ version that leverages this functionality.

Item breakdown

1. Create Rust bindings for iOS secure-enclave interactions
2. Create Rust bindings for Android KeyStore / StrongBox via JNI
3. Adding HSM support to Askar
4. Integrating HSM support into AFJ

Initiative 4: SD-JWT Module - € 21.750

Selective Disclosure for JSON Web Tokens (SD-JWT) is a specification for issuing and verifying JSON Web Tokens (JWTs) that allow for selective disclosure of claims. This means that the holder of an SD-JWT can choose to disclose only certain claims to a relying party while keeping other claims hidden.

The ARF has adopted this credential format for remote verification flows.

Relevant specifications:

- Selective Disclosure for JWTs (SD-JWT)
- SD-JWT-based Verifiable Credentials (SD-JWT VC)
- Securing Verifiable Credentials using JOSE and COSE (VC-JOSE-COSE)

Outcome

A pluggable module for Aries Framework JavaScript that allows for the creation, disclosure, and verification of SD-JWT credentials.

Item breakdown

1. Development of a generic SD-JWT library for TypeScript.
2. Creation of an SD-JWT module and integration with the library mentioned above.
3. Adding support for the `vc+sd-jwt` credential format to the Sphereon libraries.
4. Update OpenID-Client and OpenID-Service modules to support the `vc+sd-jwt` credential format..

Process Timeline

Date	Milestone	Status
July 2023	Write overall proposal	✅
01-08-2023	Finalize timeline and cost	✅
Begin August 2023	Promote proposal	✅
August - September 2023	Onboard initial partners	✅
Begin September 2023	Start initial work	✅
Februari 2024	Start work HSM work package	
Februari 2024	Finalization SD-JWT and OpenID4VC work packages	