Login with IOTA using OpenID Connect standards

Request for Proposals

Ecosystem Development Fund (EDF) - IOTA Foundation
Berlin, Germany

Contact Person: Jelle Millenaar
Email: Jelle.millenaar@iota.org

RFP issuance date: 9th of March 2022
RFP submission deadline: 19th of April 2022

Purpose

This Request For Proposals (RFP) is issued by the IOTA Foundation to encourage the development of a login system utilizing the OpenID Connect standards and the IOTA Identity framework. The IOTA Identity framework is a Self-Sovereign Identity (SSI) framework that implements the “iota” Decentralized Identifiers (DID) method, registered in the W3C DID registry, and implements other SSI concepts such as verifiable credentials and secure private key management. The DID W3C standard allows a user to create and manage their own digital identity with unique identifiers, combined with cryptographic keypairs and metadata. This makes the technology suitable for passwordless authentication, as users can provide cryptographic proof that they control an identity.

Many websites use the OpenID Connect standard from the OpenID Foundation to facilitate Single Sign-On (SSO) through a federated identity, such as a user's Facebook, Google or Twitter account. This system, which we refer to as “Web2 SSO”, is centralized around big tech providers and has been detrimental to the privacy of users. Utilizing DID, the Web2 SSO system can be recreated by developing and hosting an identity provider that implements DID. Because the provider is directly tied to a domain, it remains a centralized component; however, this approach allows multiple providers that utilize SSI to coexist. In addition, we aim to establish the identity provider as a blind participant, which logs and stores little to no information about the users while maintaining user convenience. This system would enable easy adoption as adding a new identity provider to a website can be done in mere minutes (since the implementation adheres to well-established standards).

In addition, the OpenID Foundation has been developing the Self-Issued OpenID Connect Provider (SIOP) standard to allow completely decentralized SSO and exchange of verifiable credentials. This “Web3” SSO system is much better suited to SSI since it is truly decentralized; however, it requires adopters to implement a new login system, hindering adoption. The standard is still in development, but an early implementation would allow more innovative and privacy-focused websites the ability to enjoy all SSI benefits, while fully respecting the privacy of their users.

This RFP encourages applicants to deliver a plan for the development of either a Web2 SSO system, Web3 SSO system or both, built on the IOTA Identity framework. The resulting software must be made open-source on GitHub under the Apache 2.0 license. Any implementation must be compatible with the OpenID standards and aim for maximizing security, privacy and application stability. Software quality according to ISO/IEC 25010 should be considered for the architecture and implementation of the solution.

For the Web2 implementation, support of Dynamic Client Registration is required to automatically onboard implementers. No user application will be required beyond proving that the provided solution works in a demo.

About the IOTA Foundation

The IOTA Foundation is the global not-for-profit foundation behind an ecosystem of open-source digital infrastructure in the blockchain and cryptocurrency space, including its distributed ledger technology (DLT) known as the Tangle, an incentivized staging network called Shimmer, and Assembly, a network for permissionless smart contracts.

The Tangle is an open, feeless and scalable distributed ledger, designed to support frictionless data and value transfer with the goal of being the most reliable DLT infrastructure for Web3 applications and digital economies. As a robust network for exchanging value and data between humans and machines, it is the first distributed ledger built for the Internet of Everything. The Tangle is highly scalable, allowing transactions to be added in parallel unlike blockchain alternatives; it also boasts low resource requirements, as well as zero-fee and fast transactions with finality within seconds.

Visit www.iota.org for more information.

Technical Requirements

As described in the Purpose section, this RFP has two different directions which can be explored individually in an application, or combined. In either case, a working implementation must be included for the solution(s), but will not require a focus on client applications as the solution will likely be integrated into one of our open-source wallets. Above all, the solution(s) must have a high focus on privacy, security and a frictionless user experience. We are open for submissions using all programming languages and dependencies, as long as it fulfills the requirements and goals of the RFP. Wherever possible and deemed appropriate, we have a slight preference towards Rust.

Web2

By using the OpenID Connect standard, the Web2 login allows websites to easily enroll into this new system. Onboarding new websites requires a simple addition of the identity provider to their configurations and registration at the identity provider. We suggest the identity provider be a separate piece of the solution that can be deployed by anyone. The provider may be built on existing identity provider software, such as Keycloak, Gluu or Ory. Please defend why this would be necessary in your submission.

The ideal design for the identity provider would make it completely blind. This means it does not track or log any data more than is necessary.

The identity provider's functionality must be minimized, where it outsources most tasks to the wallet component of the user. The user should be prompted in their wallet if they would like to login into the website, the information needed to grant permission must be part of the request. Any subsequent logins into the same website may be automatically accepted by the wallet, creating an SSO experience. As a bonus, verifiable credential sharing support over the established channel following the OIDC claim principle could be added.

An RFP response for a Web2 login must have the following components and requirements:

- Identity provider
  - Follow ISO/IEC 25010 and be production-ready
  - Preserving privacy by minimizing data storage and storage time
  - Able to verify DIDs from the "iota" method using the IOTA Identity framework
  - Able to verify Verifiable Credentials / Verifiable Presentations using the IOTA Identity framework for "standard claims"
  - Implement Dynamic Registration
  - Optional: Implement the OIDC claim principle
- User Architecture
  - Design how user software interacts with the identity provider
  - Implement reference implementation of the design
  - Reference implementation preferably not as web-wallet or browser extension
- Proof-of-Concept (PoC)
  - A full PoC showing how a user wallet interacts with the identity provider
  - Authentication and standard claim sharing
  - Basic relying party example

Web3

The Web3 login must be built on the Self-Issued OpenID Provider (SIOP) standard in development by the OpenID Foundation. It should follow the standard in order to enable a direct login from an edge device without the need for any centralized component, such as an identity provider. The set-up must focus on privacy and security first, making a login untraceable for any party but the relying party.

The user experience should equal the Web2 solution discussed above. This includes a basic wallet and the accompanying SSO experience as a reference implementation. This solution may also be extended with verifiable credential sharing support as is part of the SIOP standard in development.

As part of the Web3 login, a tool/library should also be created for the relying party to integrate the technology into their own systems as a reference implementation. This tool/library should focus on ease of adoption and be applicable to as many websites as possible.

An RFP response for a Web3 login must have the following components and requirements:

- User Architecture
    - Design how user software interacts with the relying party following SIOP using the IOTA Identity framework
    - Extend with OpenId Connect for Verifiable Presentations
    - Implement reference implementation
    - Preferably follow ISO/IEC 25010 and be production-ready
- Relying Party Architecture
    - Design how relying parties interact with the user following SIOP using the IOTA Identity framework
    - Extend with OpenId Connect for Verifiable Presentations
    - Implement reference implementation
    - Preferably follow ISO/IEC 25010 and be production-ready
- PoC
    - A full PoC showing how a user wallet interacts with a relying party
    - Authentication and Verifiable Presentation sharing

Submission Information

The RFP is open for submissions from the 9th of March 2022 until 23:59 CET on the 19th of April 2022. Please submit the RFP response to jelle.millenaar@iota.org and mark.schmidt@iota.org. Valid submissions will be notified no later than the 13th of May 2022. The IOTA Foundation holds the right to reject all applications if no applications fulfill the requirements according to the reviewers. Similarly, multiple applicants may be chosen to build individual implementations or components.

Submissions are allowed from most countries in the world, except for the countries deemed "high-risk" by the European Commission, Russia and Belarus. Individuals, SME organizations or non-profit organizations may all apply. Accepted applications will have their development supported by the Ecosystem Development Fund (EDF) managed by the IOTA Foundation and will be paid at milestones of their provable progress with a maximum of 10% upfront if required. The EDF will pay out milestones in IOTA tokens based on the exchange rate at the time of sending.

Proposal Format

The proposal should contain the following:

- Introduction
    - Summarize what you propose to do and how you are going to meet the goals.
- Project Proposal
    - Provide background information, including about you or your team and the specific goals you hope to accomplish. You may also include the results of any

    related research, project history or additional factors that are important to note, such as technology or economic trends.
    - Describe the architecture and technology choices and justify them.
    - Describe how your qualifications and background make you and/or your team an ideal candidate to tackle this project.
- Rationale
    - Describe your reasons for developing the project as you have proposed it. You may need to justify why you have chosen your unique approach. Consider including how your project leads to the most effective road to adoption.
- Technical/Project Approach
    - Describe the details of how the project will be managed from start to finish. This will include your specific methodologies for completing deliverables, communications with the IOTA Foundation and methods to evaluate and mitigate risk.
- Project Deliverables
    - A list of all project deliverables to be completed in the project's scope.
- Timeline for Execution
    - Summarize the timeline of project-related events from start to finish.
    - You may include a reasonable list of (optional) milestones, intermediate deliverables, that can be delivered and used to trigger partial payments.
- Budget
    - Expected expenses
- Conclusion
    - A final chance to summarize your application and make your argument

Selection Criteria

A submission is deemed valid if it is submitted before the deadline and follows the correct format. The submission will be reviewed by the EDF board and a set of technical experts based on the following criteria:

- Technical soundness of the proposed solution
- Focus on privacy and security
- Ease of adoption and likelihood of reaching short-term adoption
- Scope of the project
- Relevant expertise in the team
- Budget

We wish everyone the best of luck with their applications and look forward to hearing from you.