Commissioned by:

Guidance on Implementing Verifiable Credential Issuance

Annie Bailey

November 5, 2024

WHITE PAPER

The organization interacts with many users including employees, customers, suppliers, and contractors. In order to flexibly and securely handle the variety of each user's digital journey in an interoperable way, organizations must shift to more user-controlled methods. OpenID for Verifiable Credential Issuance (OID4VCI) is an emerging standard that bridges the gap between a new model of digital identity interaction and the known and often already implemented standards.

The scope of this paper is to provide guidance to Identity and Access Management (IAM) and security architects on implementing OIDC4VCI. This whitepaper provides context for the user-controlled model, separates hype from reality, and identifies early learnings for organizations that are ready to issue verifiable credentials.

Contents

Figures

Introduction

Identity management has moved beyond just identity for the standard personas of employees or customers. Digital identity is about everything – partners, suppliers, devices, services, and even "things". Each needs an identity, and to mesh with the modern organization, their user journey must be flexible, privacy-forward, secure, interoperable, and increasingly user-centric. While KuppingerCole's Identity Fabric illustrates the ways other IAM tools and capabilities help organizations meet these needs, there is one specific capability to address the rising user-centric need: verifiable credentials.

A verifiable credential is a digital, tamper-evident claim about a subject. Verifiable credentials are typically held by the subject (the holder), and can be digitally presented by the holder to other parties (verifiers) without having to involve the credential issuer. Verifiable credentials place the user in control of the information shared with other parties.

The user-controlled digital identity model allows an individual – be it consumer, employee, or other persona – to hold digital credentials and present them to another party, even if that party did not issue the credentials, meaning that issuing and presenting verifiable credentials do not require a pre-existing relationship between issuer and verifier or relying party. When verifiable credentials are issued according to best practice specifications like OpenID for Verifiable Credential Issuance (OID4VCI), they are secure, verifiable, privacy-protecting, and portable. An organization doesn't need to start from scratch every time it interacts with a new persona or organization.

When verifiable credentials are issued according to best practice specifications like OpenID for Verifiable Credential Issuance (OID4VCI), they are secure, verifiable, privacy-protecting, and portable.

There is quite a bit of hype around verifiable credentials and user-centric digital identity, including technology solutions with unproven track records. But there are tangible projects and initiatives that lay out the architectures for common use cases, agree on and test open standards, ecosystem requirements, and integrations between the issuer, holder, and verifiers. This is a dynamic market where – unusually – regulation and technology development are propelling each other forward; user-controlled, verifiable credential technology is developing to realize forward-thinking regulation like the European Digital Identity (EUDI) Regulation, which came to be because of advances in user-controlled digital identity technology. The EUDI regulation mandates that Member States offer digital wallets for holding verifiable credentials to residents for public and private sector use, creating an entirely new user-controlled market for digital identity issuance and exchange.

> For organizations that see the potential in issuing verifiable credentials, tapping into the benefits of cost savings, efficiency gains, privacy-enhancements, and improved user experiences, OID4VCI is the place to get started.

For organizations that see the potential in issuing verifiable credentials for the emerging user-centric ecosystem, tapping into the benefits of cost savings, efficiency gains, privacy-enhancements, and improved user experiences, OID4VCI is the place to get started. It is an open standard designed for organizations that already use OpenID to easily issue verifiable credentials based on IETF SD-JWT VC, W3C VC, ISO/IEC 18013-5 for mobile driving licenses, and other formats. It bridges the gap between a new model of digital identity interaction and the known and often already implemented standards.

For guidance, look to those working on the front lines of user-centric digital identity. Organizations like Authlete have actively contributed to key specifications like OpenID for Verifiable Credential Issuance (OID4VCI), and have built support for OID4VCI into their API authorization solutions, and tested it with the numerous wallet providers participating in the EUDI Wallet large-scale project Potential and others around the world.

Highlights

- Modern digital identity management must be flexible and secure to handle diverse personas, including user-controlled models.
- The user-centric digital identity market is uniquely evolving because regulation and technology development are propelling each other forward.
- The user-controlled digital identity ecosystem has the benefit of cost savings, efficiency gains, privacy-enhancements, and improved user experiences.
- Organizations interested in issuing verifiable credentials should consider OpenID for Verifiable Credential Issuance (OID4VCI).
- Organizations ready to start issuing verifiable credentials don’t need to reinvent the wheel – learn from those already doing it.

Definitions and Abbreviations:

- DID: Decentralized Identifier
- DIF: Decentralized Identity Foundation
- EUDI: the European Digital Identity Regulation, sometimes referred to as eIDAS 2.0
- IdP: Identity Provider
- IETF SD-JWT VC: Internet Engineering Task Force, Selective Disclosure JSON Web Tokens Verifiable Credentials

- ISO/IEC 18013-5 mDL: International Standards Organization, Mobile Driving License
- mDL: Mobile Driving License
- NIST: National Institute of Standards and Technology
- OID4VCI: OpenID for Verifiable Credential Issuance
- OID4VP: OpenID for Verifiable Presentation
- SIOP: Self-Issued OpenID Provider
- VC: Verifiable Credential
- W3C VC: World Wide Web Consortium Verifiable Credentials

The Fast-Approaching Future – Improved, Secure User Journey

> OpenID for Verifiable Credential Issuance (OID4VCI) is a protocol that defines APIs and the corresponding OAuth2-based authorization mechanisms for the user-centric issuance of Verifiable Credentials, meaning that individuals and organizations can issue Verifiable Credentials that are portable, verifiable, and do not necessitate that pre-existing relationship to present them.

The organization must come to terms with the fact that everyone and everything has an identity. KuppingerCole's Identity Fabric, depicted below, highlights this phenomenon with the identity types listed in the far-left column; consumers, customers, partners, the workforce, services, devices, and things all must have identities that interact with digital services, applications, platforms, infrastructure, backend services, and legacy IT as seen in the far-right column. These identities of everyone and everything, to everywhere must be managed in a cohesive IAM strategy, depicted by the capabilities, services, and tools in the center of the Identity Fabric.

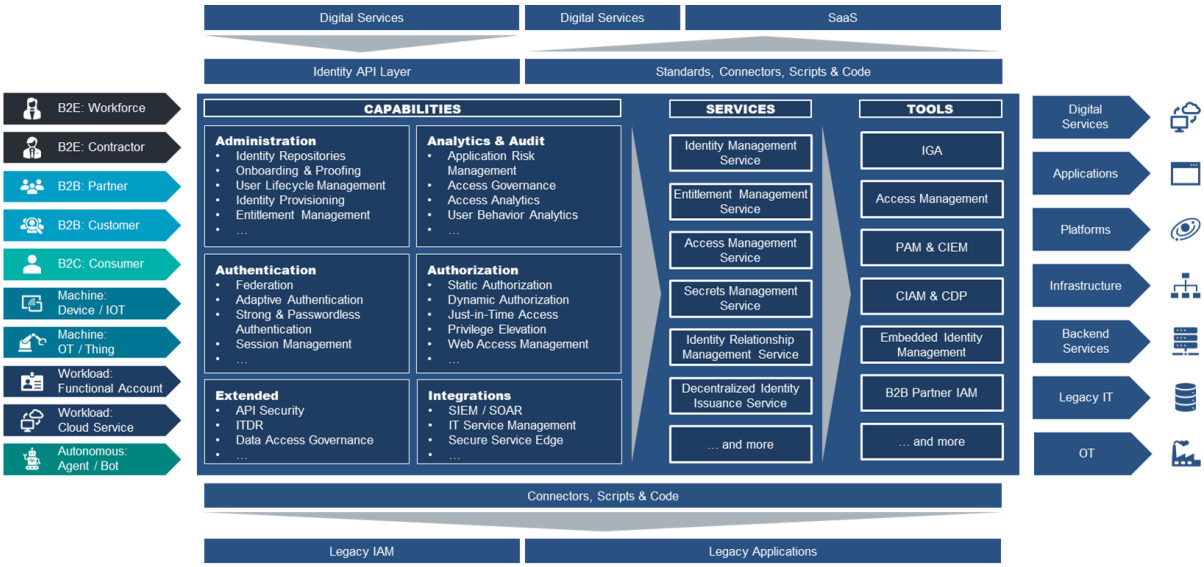

Figure 1: The KuppingerCole Identity Fabric

This is a staggering amount of complexity that must be managed securely, but allow the flexibility for each of the personas, from consumers to workforce to things, to have the adequate access to work and do business.

A key factor to success is the user journey of each persona. The user journey takes the individual from being an unknown to being known to the organization. The first interaction a persona has with an organization is typically onboarding, and repeat interactions typically require authentication.

However, each persona has different requirements, and may need to fulfil different requirements to interact with the organization. Consumers may be able to follow Bring Your Own ID (BYOID) concepts, while partners need to undergo identity verification and a credentials check. This requires the organization to be technically flexible, ready to accept different verified credential types and support onboarding for different use cases and personas.

The same goes for authentication, where personas that engage in a low-risk transaction authenticate at a lower level of security, but high-value transactions initiate step-up authentication or even a remote identity verification flow. This flexibility leads KuppingerCole Analysts to call this a deconstructed user journey, where the steps to interacting with the organization are adapted to the persona and situation.

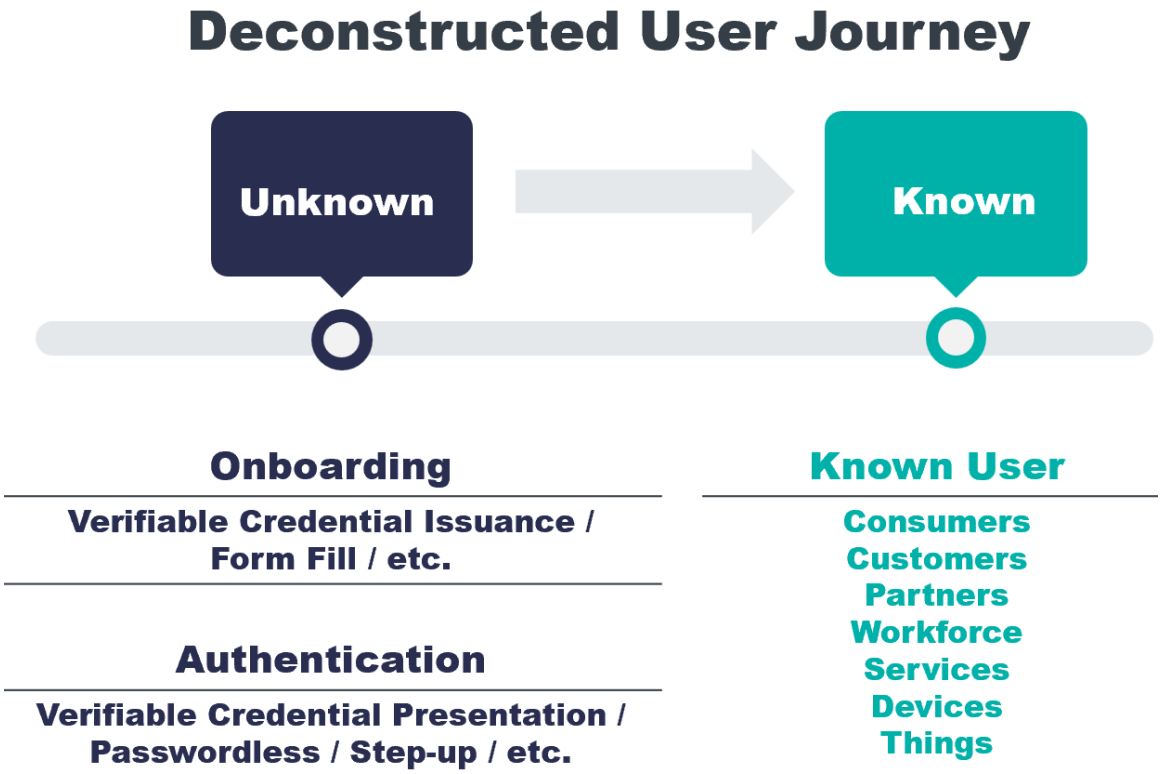

Figure 2: The deconstructed user journey summarizing flexibility for many identity personas to go from being unknown to being known to the organization

The user journey is not just a “nice to have” option. It is a must, because it brings in new business for the consumer and client personas through reduced drop-off and account opening abandonment. It wins back lost time for employees, partners, suppliers, services, devices, and things when onboarding time is reduced while increasing the security through additional credential validation or identity verification. Fraud is reduced by introducing more flexible and step-up options to authenticate customers.

Organizations do not need to reinvent the wheel themselves. Standards organizations that work towards global, open systems for digital identity provide the building blocks to a deconstructed user journey. Digital identities that follow standards such as OpenID allow for secure authentication and authorization processes, minimizing the need for multiple logins and reducing the risk of password-related breaches through contributions such as Single Sign-On (SSO), delegated access, and granular permissions. But this is not the whole story. The OpenID Foundation is standardizing a collection of open specifications for Verifiable Credentials, including issuance and verifiable presentation that elevate the user journey to a new level, opening up the realm of possibilities to include user-controlled models.

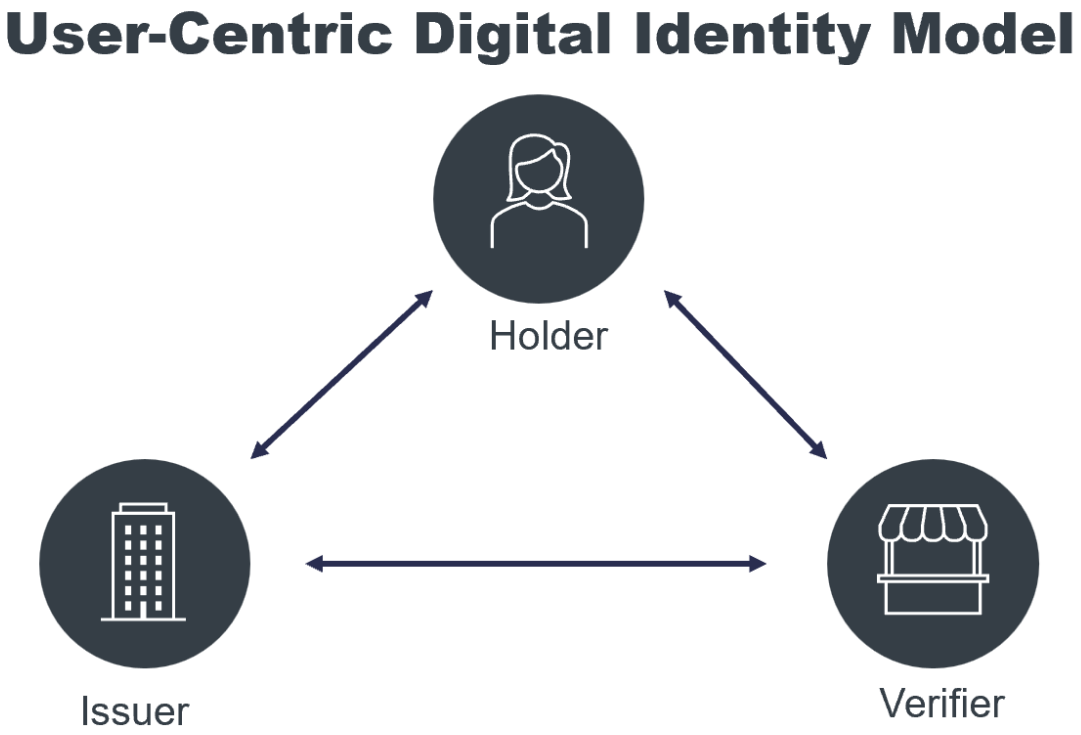

Figure 3: The user-controlled digital identity model that enables any party to assume any of the three roles

The user-controlled phenomenon enables any party to assume the roles of issuer, holder, or verifier. This includes the different personas discussed in the identity fabric (customer, consumer, workforce, partner, supplier, etc.), but also the organization to assume the role(s)

of issuer, holder, and verifier. This model enables dynamic trust to exist around the verifiable credentials that are issued and presented; an organization can issue verifiable credentials to an individual, which can then be presented to another organization to be verified. Trust is established in a quick presentation/verification process.

Traditionally, organizations that need to onboard an unknown or unregistered individual (for example, a new customer, employee, or partner) require a pre-existing relationship with that individual using traditional Identity Providers (IdPs). If a pre-existing relationship is not in place, they need to start from scratch collecting and verifying all the necessary information to onboard, often wasting time and money for both parties. In this traditional model, the organization must leverage information from traditional IdPs or do the groundwork themselves, missing out on the dynamic trust element.

OpenID for Verifiable Credential Issuance (OID4VCI) is a protocol that defines APIs and the corresponding OAuth2-based authorization mechanisms for the user-controlled issuance of Verifiable Credentials, meaning that individuals and organizations can issue Verifiable Credentials that are portable, verifiable, and enable them to be presented to another organization to be verified and, if sufficient, trusted. The user-controlled model does not require an intermediary such as a traditional IdP, but it does build on known protocols such as those from OpenID Foundation to fit seamlessly with the architecture already in place in many organizations.

Issuing Verifiable Credentials – What is Reality, and What is Hype?

> Hype is a hyper-focus on blockchain, solutions inflated on venture-capital, and abstract use cases. The way forward is with open and interoperable standards, flexible storage models, and tested use cases that solve actual business needs.

There are concrete steps that organizations can take to begin their user-centric digital identity journey. However, separating the best practices and next steps from the general hype is sometimes challenging. This paper sets apart the most relevant standards to include when setting up Verifiable Credential issuance and acceptance, how momentum is developing differently in Europe and the US, and building a bridge between standards and the business case of verifiable credential issuance and exchange.

User controlled credentials may be locally hosted on an end-user device, utilize cloud components, or completely run in the cloud. Early discussions of “decentralized identity” hyper-focused on using blockchain technology, but this was a limiting factor. The emerging standards and initiatives that are currently being developed work to enable a user-centric model that supports various credential storage options.

The major standards that organizations should be aware of are from OpenID Foundation, IETF, W3C, DIF, ISO, and NIST. This is a curated list of the current and emerging standards, but is not exhaustive.

- Self-Issued OpenID Provider (SIOP): Standard that enables a Relying Party (RP) to trust assertions made by the issuer (also an OpenID Provider) of identity information (authentication and/or claims). End users who are Self-Issued OpenID Providers (SIOP) can authenticate themselves with Self-Issued ID Tokens and present self-attested claims to RPs. This allows end users to interact with RPs without RPs needing to interact with issuers.
- OpenID for Verifiable Credential Issuance (OID4VCI): Standard that defines an API used to issue verifiable credentials in IETF SD-JWT VC, W3C VC, ISO/IEC 18013-5 mDL and other formats.
- OpenID for Verifiable Presentations (OID4VP): End users with a verifiable credential can present these to verifiers. This specification extends OAuth 2.0 to enable the presentation of verifiable credentials in SD-JWT, W3C, ISO/IEC 18013-5 and other formats.
- W3C Decentralized Identifiers (DIDs): DIDs are decentralized identifiers that can be decoupled from centralized registries, identity providers, and certificate authorities.
- W3C Verifiable Credentials (VCs): A verifiable credential is a more tamper-evident and trustworthy digital credential consisting of information about the subject, issuer, evidence on how the credential was derived, and constraints of use (expiration date, etc.).
- ISO/IEC 18013-5:2021 mDL: Specification that defines the format and contents of mobile driving licenses and methods for in-person presentation to verifiers with selective disclosure.
- IETF SD-JWT VC: Format that can be leveraged to create a selective disclosure-enabled verifiable credential.
- DIF Universal Resolver, Didcomm Messaging, Presentation Exchange, DID-JWT (& VC): Several developing standards from the Decentralized Identity Foundation for practical pieces of a user-controlled architecture.
- NIST 800-63-4: Guidelines specific to identity, authentication, and federation assurance levels and identity proofing to achieve those levels. The latest draft includes user-centric language, laying a foundation to align identity proofing with user-held wallets and credentials.

There is momentum gathering around the EUDI regulation and the large-scale pilot projects for EUDI Wallets, which include verifiable credential issuance. These showcase tangible steps towards a European-wide digital identity framework. This contrasts with the slower start in the US, which is currently more focused on specific use cases like issuing mobile driver's licenses (mDL, mDoc). The efforts of these two regions are being united in emerging standards, such as OID4VCI, which enables organizations to issue credentials according to

the prevailing formats around the world, including SD-JWT VC, W3C Verifiable Credentials and mDLs.

There are many use cases for issuing and verifying verifiable credentials, and arguably the most mature ones were tested in the large-scale pilot Potential: eGovernment services, bank account opening, SIM card registration, mobile driving license, qualified eSignature, and ePrescription.

Learnings from the Front Lines

> Some learnings are only possible from practical application. Organizations that have participated in pilot projects with successful results have particularly interesting findings.

Large-scale pilot projects such as those from the EUDI Wallet project aim to develop interoperable national digital wallets, test them for particular use cases, and refine the architecture and processes required to execute this smoothly and securely. The organizations that participate in these projects have gained valuable insights into the potential and challenges of implementing a user-centric identity model, including verifiable credential issuance. Key learnings include customization in authorization flows, selective disclosure, and the integration of other emerging standards like ISO mDL.

A key learning from these pilot projects is the importance of managing customized authorization flows, especially in the context of Verifiable Credential issuance. For example, OID4VCI uses customized scope values for Verifiable Credential issuance. OAuth2 and OpenID Connect (OIDC) play crucial roles in these flows, but they might drop customized scope values if these are not pre-registered with the authorization server. A more detailed explanation of this can be found in section 2.2.5 of OpenID for Verifiable Credential Issuance. The organizations that are participating in standards writing and pilot projects pay very close attention to configuration and pre-registration of all necessary scopes to ensure that critical authorization parameters are preserved throughout the transaction. As organizations prepare to scale their digital identity solutions, understanding and addressing these nuances in OAuth2 and OpenID configuration will be crucial for maintaining the integrity and functionality of authorization flows.

Selective disclosure is emerging as a valuable addition to the digital identity landscape. The current best practice is to use Selective Disclosure for JWTs (SD-JWT). Selective disclosure refers to the ability of a holder to choose to share only certain parts of a Verifiable Credential's information, and helps organizations to adhere to data minimization practices. Workflows to use SD-JWT with OID4VCI are already defined, and can be found in section 2.6 of OpenID for Verifiable Credential Issuance. The flow below outlines the steps to create an SD-JWT summarized as: extract a claim of name and value, add an arbitrary salt to it, and create a JSON array, encoded in base64url that yields the disclosure, and an issuer-

signed SD-JWT. This best-practice of using SD-JWT to generate selective disclosures allows data to be hidden from the Verifier without invalidating the cryptographic signature of the credential when it is presented to a verifier.

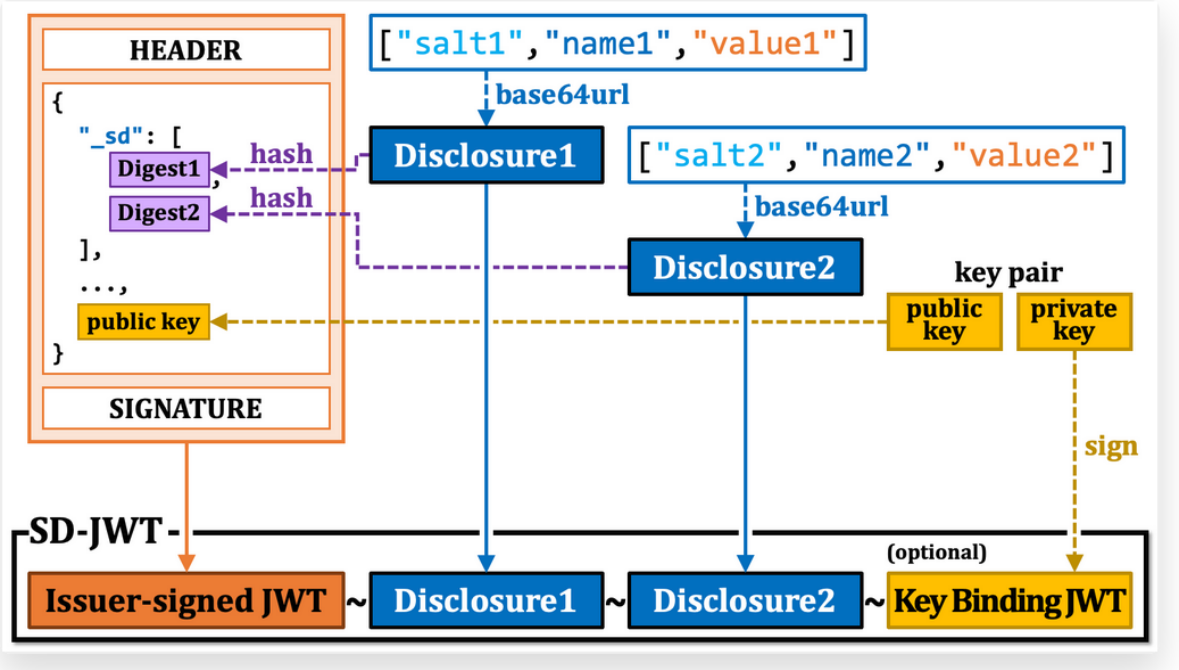

Figure 4: Using SD-JWT to create selective disclosure for a verifiable credential, section 2.6 of OpenID for Verifiable Credential Issuance courtesy of Authlete

Another critical learning is how to achieve interoperability between the systems of different businesses, industries, and countries. OID4VCI defines an API that is used to issue verifiable credentials in various formats, including SD-JWT VC and mDL as defined in ISO 18013-5. The ISO mDL specification, which standardizes mobile driver's licenses, is the standard around which momentum is gathering in the US. Organizations aiming to deploy digital identity solutions at scale must prioritize interoperability between common standards, ensuring that their systems can effectively issue and accept credentials in different formats. It is a huge benefit that the OID4VCI does not prescribe one particular verifiable credential format, but keeps it open to include the variety of options that will be globally available.

These learnings come from running pilots with the vendors that have or intend to launch products on the market. These products include wallet solutions, solutions for issuing credentials, and for verifying them.

Recommendations: Practical Advice on Implementing Verifiable Credential Issuance

Organizations should consider moving towards a more flexible, deconstructed user journey, with verifiable credential issuance being a huge opportunity for privacy-protecting, secure, and open interaction with consumers, and with every persona on the Identity Fabric.

- Surround yourself with knowledgeable partners. Just because verifiable credentials are new to your organization – and to the world – doesn't mean they are new to everyone. Select partners to work with who have hands-on experience with implementing and designing these systems. They will be able to give quick hints on what needs to be customized and what you should look out for. They already know what is ambiguous or contradictory between standards. Partners that are in the know can keep you informed of the inconsistencies, and may have solutions already worked out.

For verifiable credential issuance, Authlete is one such partner. Authlete members have actively participated in developing the OID4VCI specification, and its solutions already support it, allowing organizations to issue verifiable credentials according to the latest best practices. They have participated as a credential issuer in both the large-scale pilot Potential for the EUDI Wallet initiative and in the Global Assured Identity Network proof of concept. This means that Authlete successfully issued verifiable credentials in various formats to the many wallets participating in these projects. Integrations to the wallets were easy to facilitate.

- Offload complexity to focus on functional aspects. Issuing verifiable credentials is still quite an abstract exercise for organizations that want to be early participants in the user-controlled digital identity ecosystem. Working with a service-oriented architecture can help to offload the burden of protocol processing and token lifecycle management.

  One of the key advantages of Authlete's offering is its ability to handle OAuth and OIDC protocol operations in a dedicated backend service.

  Developer-centric solutions like Authlete simplify the implementation of API authorization and identity federation services. By providing a set of APIs that can be integrated into any form of architecture, Authlete enables developers to offload the burden of OAuth and OIDC protocol processing and token lifecycle management efficiently. This approach is particularly advantageous for organizations seeking a modern API-driven solution to handle complex authorization scenarios across various industries. Support for OID4VCI is included in Authlete 3.0, with a detailed explanation in their reference document OpenID for Verifiable Credential Issuance.

- Understand your requirements. Be clear in defining what the credentials you issue or accept must include. The essential functions of a verifiable credential are its verifiability, key binding, and selective disclosure. Build the user journey with the digital identity in mind.
- Implement the relevant standards to ensure interoperability and aligning to the developing best practice. For credential issuance, consider the current best practice standards, like OID4VCI based on SD-JWT VC, W3C VC, or ISO/IEC 18013-5 requirements.

Authlete's strength in delivering API authorization in complex, multi-party environments is an advantage in the next endeavor: issuing verifiable credentials for the user-centric digital identity ecosystem.

The potential for innovation with user-controlled identities is vast for the digital business. For the organization that is ready to participate in the promising new digital identity ecosystems, the time is right to get started.

Related Research

Leadership Compass: Identity Fabrics

Leadership Compass: Identity Governance and Administration

Leadership Compass: Access Management

Whitepaper: How to Do Identity Right When Developing Digital Services

Executive View: Authlete API Authorization

Blog: Accelerating Your Digital Journey

References:

Authlete: OpenID for Verifiable Credential Issuance (2024) <https://www.authlete.com/developers/oid4vci/#26-selective-disclosure>

DIF: Decentralized Identity Foundation (2024). <https://github.com/decentralized-identity>

European Commission: European Digital Identity (EUDI) Regulation (2024). <https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation>

IETF: SD-JWT-based Verifiable credentials (SD-JWT VC) (2024). <https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/>

ISO: ISO/IEC 18013-5:2021(en) Personal identification – ISO-compliant driving license – Part 5: Mobile driving license (mDL) application <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:18013:-5:ed-1:v1:en>

NIST: SP 800-63 (2024). <https://pages.nist.gov/800-63-4/sp800-63.html>

OpenID: OpenID for Verifiable Credential Issuance (2022). <https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-10.html>

OpenID: OpenID for Verifiable Presentations (2024). <https://openid.net/specs/openid-4-verifiable-presentations-1_0.html>

OpenID: Self-Issued OpenID Provider v2 – draft 13 (2023). <https://openid.net/specs/openid-connect-self-issued-v2-1_0.html>.

W3C: Decentralized Identifiers (DIDs) v1.0 (2022). <https://www.w3.org/TR/did-core/>

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.