EPiC Series in Computing

Volume 95, 2023, Pages 311–319

Proceedings of European University Information Systems Congress 2023

A self-sovereign way to exchange educational credentials

Emmanouil Koukoularis, Vasileios Markopoulos and Nikos Voutsinas
Greek Universities Network, Greece

koukoularism@gunet.gr, billymark@gunet.gr, nvoutsin@gunet.gr

Abstract

In a time of ever-increasing digital transformation, where the amount of data transferred and verified in digital form has vastly increased, new specifications have been released, enabling the exchange of educational credentials in a privacy-respecting manner while maintaining the anonymity of the contributing parties. Hereafter a model is described for educational credentials exchange, built upon the latest W3C and OpenID Connect specifications for Verifiable Credentials and Verifiable Presentations. These emerging technologies and specifications drive the digital transformation towards Web 3.0, while universities can leverage these to provide students and graduates with a secure and self-sovereign method of sharing digital credentials, simplifying the diploma verification process necessary for job applications or when pursuing post-graduate studies. This model encompasses the core principles the next version of the digital diplomas platform of the Greek HEIs (eDiplomas) is based on.

1 Background

Until now the majority of Higher Education Institutions have been following procedures confined by the rules of a paper-based exchange of certificates. In Greece, starting with the eDiplomas platform, the digital transformation of the ecosystem has initiated as it allows for issuing of digital diplomas for graduates on behalf of the corresponding institutes. The platform allows registered organizations to access digital diplomas upon authorization of the diploma holder. Currently, the eDiplomas platform is based on a conventional architecture and Web2.0 trust model where all issuers, verifiers and holders need to trust a central authority. However, the rise of new specifications such as the W3C Verifiable Credentials (VC) and extensions of OAuth Authorization Framework, pave the road to a new security and privacy protocol and allows the decentralization of the ecosystem (Figure 1).

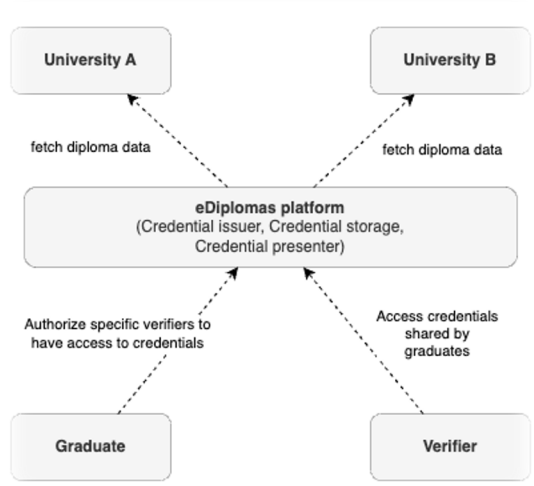

Figure 1. Centralized Model

2 Trust Framework

The first step in the transition to a more decentralized ecosystem is to decouple all the actors (Issuer, Holder and Verifier as shown in Figure 2), so that Issuers are agnostic of where the credentials of a Holder are shared to. This concept was introduced in the W3C Verifiable Credentials (VC) specification (Longley, Sporny, & Chadwick, 2022), which describes the format of a Verifiable Credential and its capabilities.

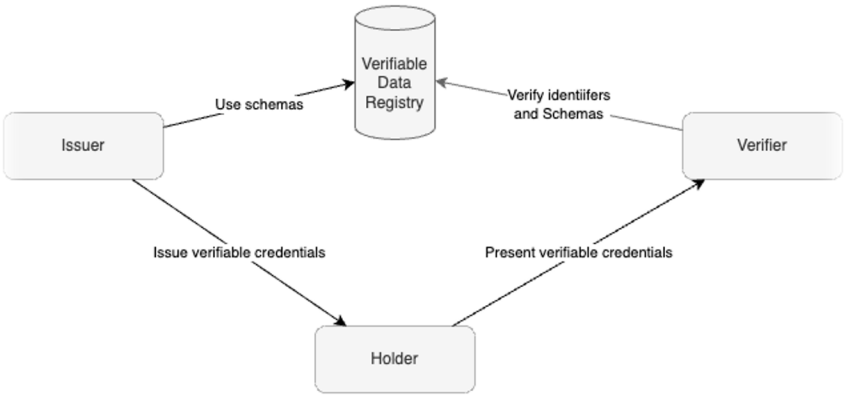

Figure 2. The trust triangle

2.1 Verifiable Data Registry

To attain the security and privacy requirements which are the primary targets of our ecosystem specification, a set of registries must be installed.

1. **Trusted Schemas List**

A JSON Schemas List will enhance interoperability between the actors, as it will ensure that they communicate with the same well-known verifiable credential schemas stored in this registry. More specifically, this registry can help the verifier define the type of credentials he wants to receive based on this registry. Some schemas which could be used as a template are namely: National ID, University Degree Diploma and the Micro-credentials schema. Note that these schemas must be well-defined and **flexible** enough to enable the end-user the ability to disclose **the smallest possible subset** of data of the issued credential to a Verifier.

2. **Qualified Issuers List**

To build trust for wallet users, each Issuer must first have been registered into the Qualified Issuers List with the associated information, such as the Public key and an Issuer portal URL.

3. **Trusted Wallet Providers List**

Many credential issuers would like to know what wallet they are issuing credentials to and how private keys are managed. To ensure trust between the Wallet Provider and a Trusted Issuer, the following mechanisms can be utilized as a criterion for the registration of a Wallet Provider into the Trusted Wallet Providers List:

- Client authentication: This mechanism enables a Wallet to authenticate with a Credential Issuer by establishing a communication channel with the wallet backend which maintains the private keys.
- App attestation: Establishes trust in the way the wallet stores the verifiable credentials.
- Key attestation: Establishes trust in the way the wallet stores the cryptographic keys (local/remote HSM).
- Device attestation: Establishes trust in the device itself, as some devices could work in a malicious way and distribute credential data to other parties without the consent of the user.

4. **Relying Parties List**

The Relying Parties List provides an additional security layer above SSL, during the presentation of claims procedure, to protect the holders from malicious undisclosed recipients (Example of Relying parties could be Banks or other legal persons).

5. **Credential Revocation List**

This list contains a set of credential identifiers which are associated with the credentials which have been revoked by trusted issuers. Various design mechanisms can be applied to make each record of the registry as compact as possible.

2.2 Identity binding with wallet keys

The first thing the end-user (student) must do to activate a wallet, is to visit a national authority **in person** in order to receive a **National ID** verifiable credential which is the first VC that will be stored in the wallet. It is crucial that the National ID is issued in a **supervised environment** to ensure that it is stored in the wallet of the correct person. From now on, the student/graduate can use his/her National ID VC to receive any other VCs, such as the university degree. The National ID verifiable credential is a credential which is issued once and can be issued again only if the previous National ID VC is revoked. The revocation of the National ID VC can only happen in case the Holder has lost access to his Wallet or the keys of the issuer have rotated.

2.3 Privacy considerations

For security reasons, issuers should adopt the policy of issuing credentials **only once** until they are expired or revoked, either by the issuer or the holder. This means that the issuers need to keep track of the credentials being issued. This policy reduces the possibility of issuing one Diploma to more than one Wallet by abusing an Issuer's web platform. The lifespan of a Diploma VC before it expires could be one year, after when the end-user would have to request the diploma again from the Issuer website. The Credential Revocation registry as described previously, should be designed in a way which does not allow malicious actors to track the holders' movements. Technologies such as Zero Knowledge Proofs (ZKP) and Multi-Party Computation (MPC) could be utilized to enhance the privacy in that matter.

3 Selective disclosure framework

By nature, diplomas contain sensitive data about the credential subject. Therefore, the ability to disclose only specific parts of the issued credential is of paramount importance for the privacy of the holder. The SD-JWT specification (Fett & Yasuda, 2022) can be implemented using the supported cryptographic and hashing algorithms described in [SOG-IS ACM] (SOG-IS Crypto Working Group, 2020). As the specification describes, the Credential Issuer sends a Holder the following:

- A signed SD-JWT, which contains a set of selectively disclosable fields in hashed format.
- A list of *Disclosure* objects, each of which contains the Salt, the Field Name and the Field Value of each selectively disclosable field.

When a Holder of an SD-JWT credential decides to selectively disclose fields of his verifiable credential to a Verifier, he sends:

- The issuer-signed SD-JWT, which contains a set of selectively disclosable fields in hashed format.
- A subset of *Disclosure* objects, each of which contains the Salt, the Field Name and the Field Value of each selectively disclosable field, so that the Verifier can have access to the value of fields selected by the Holder.

To enforce stability and interoperability into the network of the ecosystem, all actors (Wallet, Issuer and Verifier) should use the Edwards-curve Digital Signature Algorithm (EdDSA) for the signing of Verifiable Credentials and Presentations and SHA-256 when hashing is required. On Figure 3 you can see an overview of the SD-JWT issuance and verification flows.

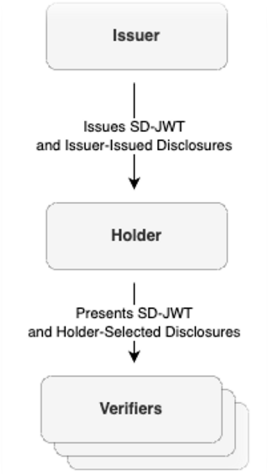

Figure 3. SD-JWT Issuance and Presentation flow

4 Transactions framework

The primary objective of storing diplomas in a decentralized digital wallet is to guarantee that graduates are in control of their own online interactions and presence, when it comes to presenting a diploma or lifelong certificate for any purpose, from applying for a postgraduate degree program, to applying for a job position without the issuer of the credentials gain any information about the transaction between the holder and the verifier.

4.1 OpenID4VCI (OpenID for Verifiable Credential Issuance)

The recently released **OpenID4VCI (OpenID for Verifiable Credential Issuance)** (Lodderstedt, Yasuda, & Looker, OpenID for Verifiable Credential Issuance, 2023) specification which extends the standardized OAuth 2 Authorization Framework [RFC6749] (Hardt, 2012) is designed in a way to maintain the security skeleton of the [RFC6749] and extend it by introducing new parameters on the endpoints of the Authorization Server.

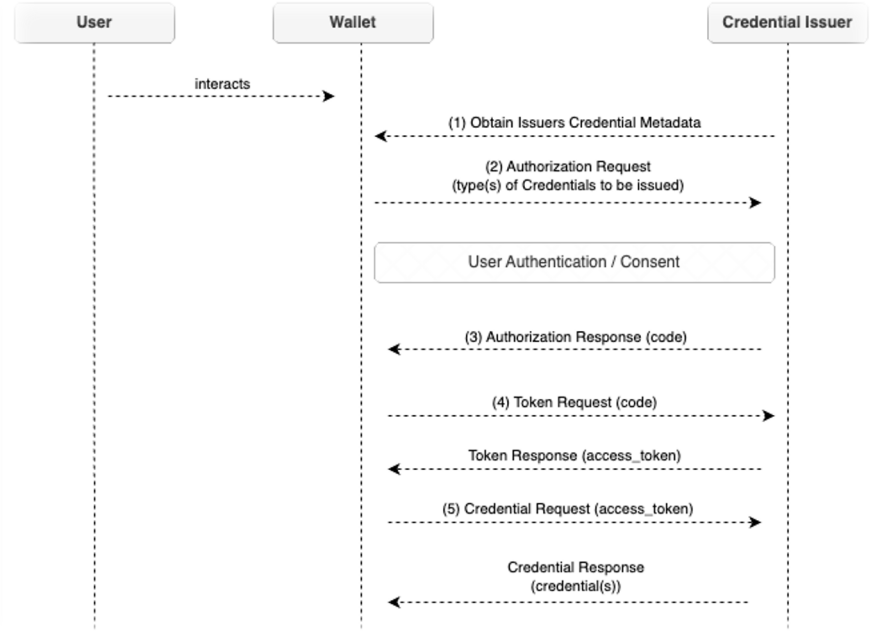

Figure 4. Authorization flow (OpenID4VCI)

Credential Issuer metadata

Apart from the endpoints of the issuer, the metadata JSON object also contains information (logo URL and color pallets) on how the issuer should be displayed on a separate application such as a wallet. The Credential Issuer metadata also contains a list of the supported verifiable credentials based on format and credential type. Additionally, each supported credential object contains similar information about how the specific credential could be displayed on a different application.

Authorization details instead of scope

In the OAuth 2 framework, for the *Client* to communicate which part of the data it wants to have access to from the *Authorization Server*, it must pass some plain `scope` names. The OpenID4VCI specification leverages the `authorization_details` parameter defined in (Lodderstedt, Richer, & Campbell, OAuth 2.0 Rich Authorization Requests, 2023) which can be used for conveying the details of the credentials (format and types) the *Wallet (Client)* wants to receive from the *Credential Issuer (Authorization Server).*

User Authentication

In today's most applications, user authentication is achieved with traditional authorization frameworks such as OAuth, OpenID Connect (OIDC) and SAML. However, in the case of receiving credentials, the *Credential Issuer* should not just authenticate the end-user, but authenticate the user through the wallet. For example, if a Diploma VC Issuing platform authenticates end-users with just OIDC, then a person who has access to the actual graduate's username/password credentials will successfully receive the Diploma VC. To tackle this problem, the user authentication mechanism should require Verifiable Credentials from the wallet in order to identify the end-user. By utilizing the already received National Verifiable ID credential described in the Section 2.2 of this paper as means of authenticating the user, the *Credential Issuer* has high level of assurance that this credential is securely received because it was issued to the wallet in a supervised issuance flow requiring the presence of the end-user. The National Verifiable ID credential should contain a personal identifier which can be used by the *Credential Issuer*

to find the corresponding diplomas for the specific end-user. The specification used for the presentation of the National Verifiable ID to a *Credential Issuer* is the OpenID for Verifiable Presentations which will be described later.

Binding the Issued Credential to the identifier of the End-User possessing that Credential
In order for the Issuer to bind the credential to the identifier of the holder (on Credential Request presented in Figure 4), the holder must provide proof of control, either alongside or without any key material. Cryptographic binding secures that the credential being presented to a verifier from an end-user, has actually been issued for that specific end-user. Keep in mind that this user identifier should match the identifier in the National Verifiable ID presented during the **User Authentication** step.

4.2 OpenID4VP (OpenID for Verifiable Presentations)

Storing Verifiable Credentials is pointless without a mechanism to exchange the information contained. The OpenID4VP (OpenID for Verifiable Presentations) specification (Terbu, Lodderstedt, Yasuda, Lemmon, & Looker, 2023) defines a mechanism on top of OAuth 2.0 [RFC6749] that enables the presentation of Verifiable Credentials in the form of Verifiable Presentations.

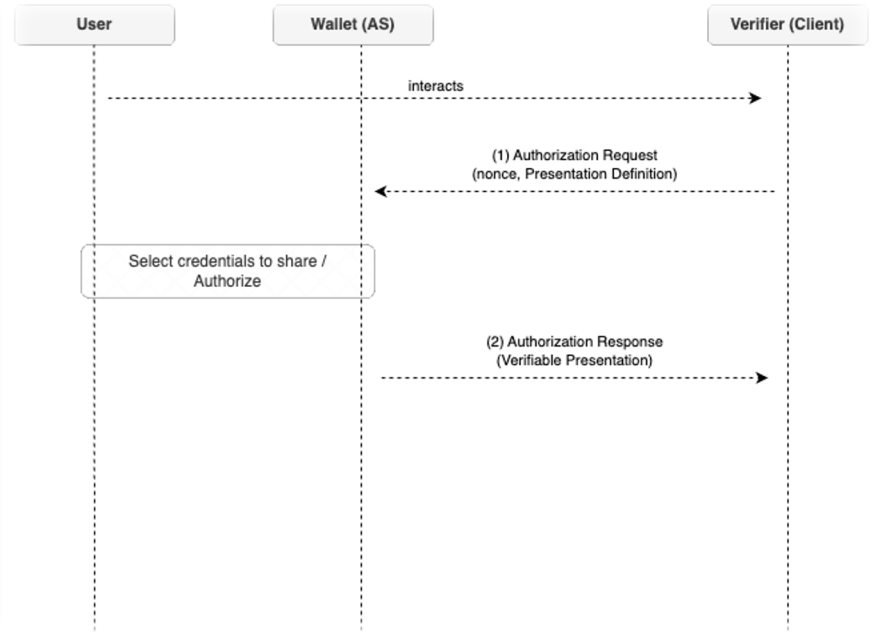

Figure 5. Presentation flow (OpenID4VP)

Authorization Request
As shown in Figure 5, the Authorization Request contains a *nonce* so that the Holder can prove ownership of the keys and a *presentation definition*

Presentation Definition
Describes the credential types or schemas or specific fields of a schema which the Verifier expects to receive from the Holder.

Authorization Response

A POST request containing a Verifiable Presentation which is encrypted/signed and contains the *nonce* passed on the authorization request.

5 Conclusion

Verifiable Credentials are the main pillar of the digital transformation of HEIs, by enabling the transition of identity systems to a self-sovereign architecture. In this digital generation, control of personal data is returned to the hands of end users, especially through the use of selective disclosure. Our study revealed the importance of a common Trust Framework, in order to achieve interoperability and avoid vendor lock-in. Universities and HEIs should adopt secure, latest-gen infrastructure, based on already secure protocols and state-of-the-art privacy-enhancing technologies, before it is too late, if they want to prosper in the ever-progressing digital wave of innovation.

Bibliography

Fett, D., & Yasuda, K. (2022, December 7). *Selective Disclosure JWT (SD-JWT).* Retrieved from IETF: https://www.ietf.org/archive/id/draft-ietf-oauth-selective-disclosure-jwt-02.html

Hardt, D. E. (2012, October). *The OAuth 2.0 Authorization Framework [RFC6749].* Retrieved from IETF: https://www.ietf.org/rfc/rfc6749.txt

Lodderstedt, T., Richer, J., & Campbell, B. (2023, January 30). *OAuth 2.0 Rich Authorization Requests.* Retrieved from IETF: https://www.ietf.org/archive/id/draft-ietf-oauth-rar-23.html

Lodderstedt, T., Yasuda, K., & Looker, T. (2023, February 3). *OpenID for Verifiable Credential Issuance.* Retrieved from OpenID Foundation: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html

Longley, D., Sporny, M., & Chadwick, D. (2022, March 3). *Verifiable Credentials Data Model v1.1.* Retrieved from W3C: https://www.w3.org/TR/vc-data-model/

SOG-IS Crypto Working Group. (2020, January). *SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms.* Retrieved from SOGIS (EU): https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

Terbu, O., Lodderstedt, T., Yasuda, K., Lemmon, A., & Looker, T. (2023, February 3). *OpenID for Verifiable Presentations.* Retrieved from OpenID Foundation: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html