NGI TRUST CHAIN

D1. 'STATE OF THE ART OVERVIEW, USE CASE ANALYSIS AND PRELIMINARY TECHNICAL SPECIFICATION OF THE SOLUTION'

OIDC-PRINCE

22/03/2024

Funded by the European Union

TrustChain Project. Funded by the European Union under GA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Grant Agreement No.: 101093274
Call: HORIZON-CL4-2022-HUMAN-01
Topic: HORIZON-CL4-2022-HUMAN-01-03
Type of action: RIA

D1. 'STATE OF THE ART OVERVIEW, USE CASE ANALYSIS AND PRELIMINARY TECHNICAL SPECIFICATION OF THE SOLUTION'

OIDC-PRINCE

Due date	22/03/2024
Submission date	22/03/2024
Team	Bruno Sousa Bernardo Arzileiro Tiago Galvão Paulo Silva
Version	1.0
Authors	Bruno Sousa Bernardo Arzileiro Tiago Galvão

Funded by the European Union

EXECUTIVE SUMMARY

OIDC PRINCE project aims to enhance the privacy support in user consents used in OpenID Connect authentication and authorization processes. Users need to be informed regarding the potential risk of providing consent for the personal information access by services/entities that may not be trusted by the user and the OpenID Provider, which is responsible to manage the authentication and authorization. OpenID PRINCE introduces the proof of privacy regulations compliance (e.g., compliance with GDPR) in the OIDC discovery and registration processes using data privacy vocabulary (DPV) specification that can be certified by entities external to the OIDC authentication process. These proofs can be stored securely in a EMV compliant blockchain. OIDC PRINCE also enables privacy analysis to assess the risk of services accessing the end-user private information. This analysis, performed by Fuzzy Logic models considers the claims which access is being requested and the profile of the service requesting the access, for instance if it is a service associated with acquisitions or a service for education and learning. OIDC PRINCE contributes to enhance the support of privacy in OpenID connect by enabling informed consents, and by minimizing the data sharing with entities that are not trusted, or that do not provide evidence of being trustworthy in terms of privacy management.

This document summarizes the solutions, standards found in the state of the art that are relevant for the goals of OIDC PRINCE.

TABLE OF CONTENTS

Funded by the European Union

LIST OF FIGURES

Funded by the European Union

LIST OF TABLES

ABBREVIATIONS

DID	Decentralized Identifier Document
DPV	Data Privacy Vocabulary
EVM	Ethereum Virtual Machine
IAM	Identity Access Management
IP	Internet Protocol
GDPR	General Data Protection Regulation
LMS	Learning Management Systems
NCS	Networks, Communications and Security
OIDC	OpenID Connect
OSP	Online Selling Platform
OWL	Web Ontology Language
PII	Personal Identifiable Information
RDF	Resource Data Format
SIOP	Self-Issued OpenID Provider
SKOS	Simple Knowledge Organization System
SSI	Self-Sovereign Identity
SSO	Single Sign On
TCP	Transmission Control Protocol

Funded by the European Union

1 INTRODUCTION

The University of Coimbra is a public higher education institution, which provides education and research and knowledge transfer activities. The Network, Communications and Security (NCS) is part of the Centre of Informatics and Systems of the University of Coimbra. The NCS has an extensive experience in research projects and security solutions targeting specific domains, like smart grids, critical infrastructures, communication networks among others.

The OIDC PRINCE project aims to enhance the privacy support in the consents of OpenID Connect authentication and authorization processes. The consent to access the end-user data (e.g., gender, birthdate, phone number, postal address, zip code) has privacy issues and does not consider the type of user that may request access to such data. Users need to be informed regarding the potential risk of providing consent to share personal information with entities that may not be fully trusted by the user, OpenID Providers, as their compliance with GDPR is not known. Solutions like OpenID Connect are the foundation of the Single Sign On (SSO) processes. Thus, it is desirable that authentication processes through OIDC, consider the GDPR compliance degree in services. In other words, policies can block services that are not compliant with GDPR, and this enforcement can be done by OpenID Providers.

OIDC PRINCE aims to fill this gap by introducing Data Privacy Vocabulary (DPV) that allows to express data in a readable form, and that includes extensions for GDPR to express compliance levels of GDPR. The proofs in DPV format can be combined with Decentralized Identifier Documents (DIDs), allowing the mapping of an entity (service identification) with its GDPR compliance. DIDs and DPV can be stored in the EVM compliant blockchain. Upon on the EVM blockchain (Alastria in the case of OIDC-PRINCE), the OpenID Provider can implement policies that consider the GDPR compliance information.

2 MOTIVATION AND PLANNED FUNCTIONALITIES

OIDC PRINCE established has the goal of enhancing the privacy support in OpenID Connect authentication and authorization processes. The risks associated with SSO processes with services that are not compliant with GDPR, or being compliant request more information than they should be in possession of. These privacy risks need to be for the knowledge of the users, especially when providing consents, that is, when allowing the access to claims. The motivation behind OIDC PRINCE is to fill the gap in privacy support in OIDC SSO processes and to promote privacy compliance.

The three goals of the project include:

- Goal 1. Foment privacy regulations compliance by introducing the proof of compliance in services aiming to access personal data. Without providing such proof OpenID providers (OP) may opt to not allow the registration of services for federated authentication processes, or to support SSO.
- Goal 2. Support informed end-user consents regarding the privacy risks and trustworthy information. Risk privacy analysis allow to objectively determine the risk of sharing private.
- Goal 3. Increase trust in relevant operations like authentication and authorization enabled in standard solutions like OpenID Connect, used to enable SSO, widely used nowadays.

From the OIDC PRINCE goals the following functionalities can be drawn:

1. Manage documents proving GDPR compliance (DPV)
2. Manage identity of services in a decentralized fashion (DIDs)
3. Policies management as per GDPR compliance levels by OpenID Provider
4. Risks analysis in consents (Fuzzy Models)

The following subsections detail each of these functionalities.

2.1 MANAGE DOCUMENTS PROVING GDPR COMPLIANCE (DPV)

Goal:

This functionality aims to allow the management of documents proving GDPR compliance using the related DPV standards.

Requirements:

- This functionality assumes that there are already DID and/or a verifiable credential for a service.

How:

The steps to produce and use the proofs are as follows:

1. The service as a specific identifier or verifiable credentials (step not in the scope of OIDC PRINCE)
2. The service is audited by trustable entities and these issue a proof that the service identified by a certain DID is compliant with GDPR. (step not in the scope of OIDC PRINCE)
3. The proof is placed in a EVM blockchain.
4. (optional) the service can add to its DID, the proof of compliance stored and issued by the trusted auditing entities.
5. The service when registering to the OpenID Connect using its DID, also presents information of the proofs of GDPR compliance.
6. The OpenID Connect by receiving such information can assess its trustworthiness by assessing the information in the EVM blockchain.
7. If the compliance with GDPR policies accept, the service is registered in the OpenID Provider. If not accepted the OpenID provider does not accept the client and may reject any future attempt of registration.

The DPV proofs are stored in the EVM blockchain and are used in the client registration of OpenID Connect, as pictured in Figure 1.

Funded by the European Union

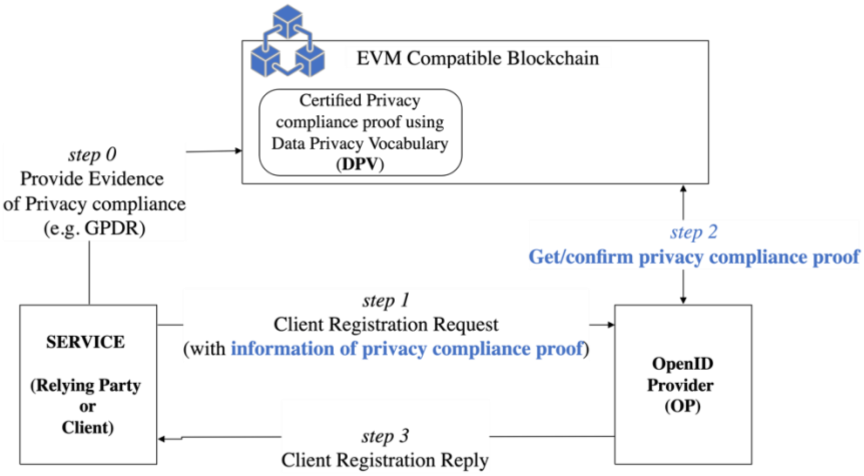

EVM Compatible Blockchain
Certified Privacy compliance proof using Data Privacy Vocabulary (DPV)
step 0
Provide Evidence of Privacy compliance (e.g. GPDR)
step 2
Get/confirm privacy compliance proof
step 1
Client Registration Request (with information of privacy compliance proof)
SERVICE
(Relying Party or Client)
OpenID Provider (OP)
step 3
Client Registration Reply

FIGURE 1 - OVERALL FUNCTIONALITY OF DPV MANAGEMENT

2.2 MANAGE IDENTITY OF SERVICES IN A DECENTRALIZED FASHION (DIDS)

Goal:

The goal of this functionality is supporting Self Sovereign Identity (SSI) using DIDs or verifiable credentials (VCs).

Requirements:

The requirements of this functionality are:

1. The service has the means to request the DID or a verifiable credential for a service that he owns or manages.
2. The user when authentication also uses a DID, instead of weak identity models like email and password.
3. The use of DIDs in OpenID connect requires the support for Self-Issued OpenID Identity Provider (SIOP) and Verifiable Credentials

How:

The DIDs can be used authenticate users, as follows (simplified view):

1. A User has a DID and stores it securely in its wallet (not in the scope of OIDC

Funded by the European Union

PRINCE)

2. A user accesses a service (which was already registered in OpenID provider) and is requested to authenticate.
3. Through SIOP the user is authenticates by using its DID.
4. The OpenID Connect Provider can confirm the identity of the user and to authenticate him.

2.3 POLICIES MANAGEMENT AS PER GDPR COMPLIANCE LEVELS BY OPENID PROVIDER

Goal:

The aim of this functionality is to allow the enforcement of policies using the GDPR compliance information, provided in DPV format.

Requirements:

The requirements include:

1. A relying party/client can present the information of GDPR compliance in a DPV format.
2. The information of GDPR compliance is stored in a EVM blockchain.

How:

The following steps occur:

6 All the steps of the functionality of Manage document proving GDPR compliance are executed, from step 1 to step 7,

7 on the step 7, the policies at the OIDC provider may:

  a. accept the client because it is fully GDPR compliant;
  b. accept the client because it is partially GDPR compliant and increases the privacy/security risk level;
  c. not accept the registration of the client because it is not GDPR compliance;
  d. not accept the registration of the client because it does not provide any proof of compliance.

Funded by the European Union

The policies are applied at the side of the OIDC provider and can accept or deny the registration of the client.

2.4 RISK ANALYSIS IN CONSENTS (FUZZY MODELS)

Goal:

This functionality determines the security and privacy risks that a user may have when providing access to its Personal Identifiable Information (PII).

Requirements:

The OpenID provider has means to determine the service type, or this information is provided by the service when registering in the OIDC provider.

How:

The steps for this functionality mainly includes the steps of the authorization code flow in OIDC, which are pictured in Figure XXX and are summarized as follows:

1. A user accesses a service.
2. The service requires the user to be authenticated using a Single Sign On (SSO) functionality.
3. Upon the authentication request the service requests access to specific resources/claims, information of the user (e.g., email, address, gender, phone).
4. The OIDC Provider determines the privacy risk associated with the requested claims.
5. The OIDC Provider informs the user of the possible privacy risks and provider a list of acceptable claims, according to the type of service (e.g., education, selling, social media, ...) and other information items.
6. The user is made aware of the risks and performs a final selection of the claims that will be accepted.
7. The OIDC Provider conveys the accepted and consented claims to the service.

Figure XX illustrates the steps that are executed, and where the risk assessment is crucial.

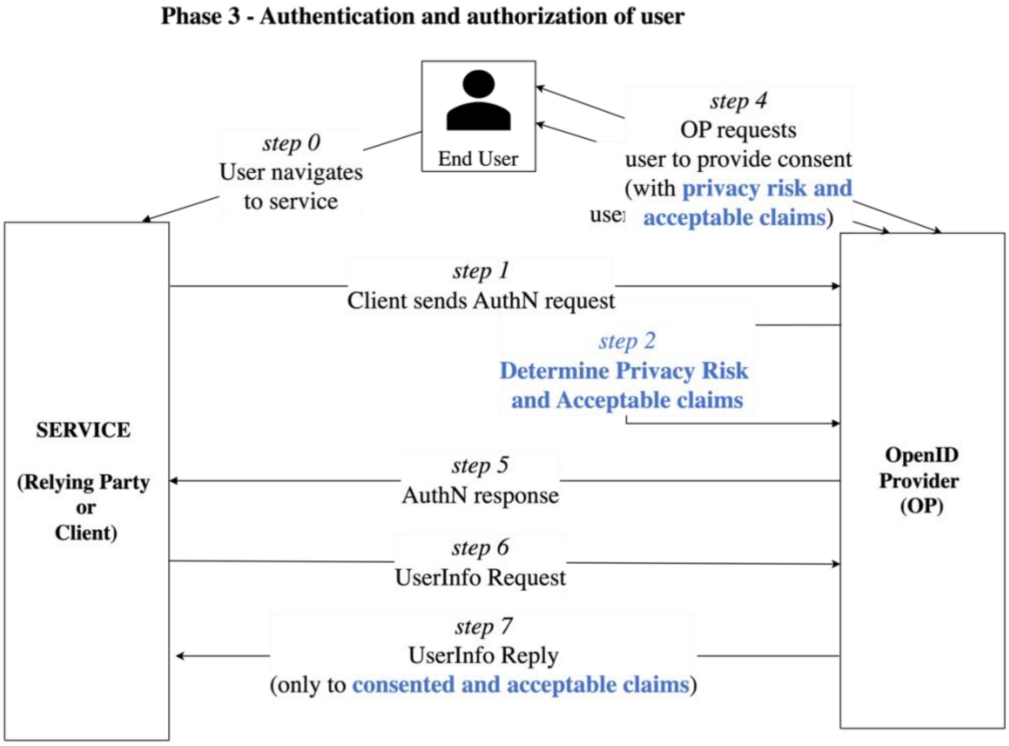

Phase 3 - Authentication and authorization of user
End User
step 0
User navigates to service
step 4
OP requests user to provide consent (with privacy risk and acceptable claims)
user
SERVICE
(Relying Party or Client)
OpenID Provider (OP)
step 1
Client sends AuthN request
step 2
Determine Privacy Risk and Acceptable claims
step 5
AuthN response
step 6
UserInfo Request
step 7
UserInfo Reply
(only to consented and acceptable claims)

FIGURE 2 - RISK ANALYSIS IN THE OIDC STANDARD AUTHORIZATION FLOW

Funded by the European Union

3 USER NEEDS ASSESSMENT

3.1 PROVIDE A DETAILED ACCOUNT ON THE RESEARCH CONDUCTED FOR YOUR COMMUNITY OF USER'S NEEDS.

The user's needs have been mainly determined based on the experience we have with SSO solutions through OIDC [1-3], and on the risk and privacy analysis we have identified in several use cases [4-6]. This led us to propose the OIDC PRINCE project proposal to the OC2 TRUSTCHAIN call.

Our findings, regarding the privacy issues in OpenID connect are also shared with other authors in the literature [7-10], which state that OpenID connect, and OAuth 2.0 protocols provide low privacy to the user, and the identity provider can gather information regarding the user web behaviour. One of the works [9] proposes extensions to prevent relying parties from tracking users, another [10] proposes an extension to consider the trust level of the OpenID provider.

Additionally, the European Union [11] has been promoting the initiative of Digital Identity for all Europeans, which besides each citizen having a digital identity recognizes anywhere in Europe, it also allows users to control how information can be shared with a service requesting such information. OIDC-PRINCE has this need in its roots, namely providing information to the users regarding the risks in sharing information with services.

The Self-Sovereign Identity (SSI) allows users to have full control of their data, instead of 'delegating' it to a third party, in this context Decentralized Identifiers (DID) and Verifiable Credentials (VC) are key technologies to support SSI. Several core foundational protocols on the Internet have been receiving support for DIDs and VCs, like OpenID Connect.

OIDC-PRINCE considers mainly two type of use cases:

- Education addresses the needs of users who want to have access to learning management systems, which provide materials for learning courses. Such systems can leverage on OpenID Connect to support federated authentication, by avoiding the user account duplication. They can perform login with the account they have in the university.
- Marketing, online selling platforms, this use case addresses the needs of users that aim to buy or sell goods online, using platforms to search, promote and buy their products. Instead of creating a user account with credentials in the selling platform, they rely on OpenID Connect to perform SSO, using their email account.

Funded by the European Union

3.2 GIVEN SUCH GENERAL TRENDS, PROVIDE WITH A PARALLEL LIST OF USER STORIES SO THE FUNCTIONALITIES OF THE TOOL GIVE RESPONSE TO THEM

This section highlights the user stories to be considered in the OIDC PRINCE developments, and evaluation through User-Centric Design of the two use cases: Education and Selling Platform.

▪ Education

This use case addresses the needs of users who want to have access to Learning Management Systems, with the following user stories.

User Story 1: Authentication

As a student I want to be able to login to the LMS using my student account, so that I'm able to have access to the learning materials, like course presentations, videos, notes from teachers, and perform exams and have access to the graduation notes.

Note: the LMS might not be integrated with the Identity Access Management (IAM) system of the University but is configured to support authentication using students accounts managed in the University IAM.

Example: The LMS can be provided by another institution and might be outside the infrastructure of the University.

User Story 2: Risk Aware Information

As a student I want to be able to have risk information when providing consent to the LMS using my student account, so that only the required data is shared with the LMS. In other words, the LMS may not need to have access to my personal address, if all the documentation is provided in a digital fashion.

Note: The LMS upon authentication of the user will request access to resources (considered claims in OpenID Connect specification) like the email account, phone number, gender, and others. The user needs to consent the access to such fields.

Example: The user should have information of risk if the LMS request access to resources that it does not require to perform its functionalities, like full details of the address, or to the information of personal websites of the user (see full resources on Table 1).

User Story 3: Trust in the authentication system

As a student I want to be able to trust in the LMS using my student account, so that have guarantees that my data is kept private. The IAM on the University needs to have a mechanism to verify the compliance of GDPR of LMS.

Note: The entities managing the IAM of the university and the LMS are different, and may take distinct approaches regarding GDPR compliance

Example: The University is fully compliant with GDPR, while the LMS is partially compliant with GDPR.

User Story 4: Proofs of GDPR compliance

As a service owner I want to be able to provide transparent proofs of GDPR compliance, so that users use my services. As a service I want to provide immutable proofs that I can comply with GDPR.

Note: I've been audited in terms of GDPR compliance, and I want to use proof of GDPR compliance to increase user trust on my service.

Example: The LMS was audited and certified in terms of GDPR compliance, such certification is held in a EVM blockchain.

▪ ONLINE Selling Platform (OSP)

This this use case addresses the needs of users that aim to buy or sell goods online, using platforms to search, promote and buy their products.

User Story 1: Authentication

As a user I want to be able to login to the online selling platform using my email account, so that I'm able to have access to the functionalities of the selling platform.

Note: The selling platform might not be integrated with IAM system of my mail services provider.

Example: The selling platform can be eBay and my IAM account can be managed by Google.

User Story 2: Risk Aware Information

As a user I want to be able to have risk information when providing consent to the online selling platform using my email account, so that only the required data is shared with the OSP. In other words, the OSP may not need to have access to my

Funded by the European Union

gender to perform its functionalities.

Note: The OSP upon authentication of the user will request access to resources (considered claims in OpenID Connect specification) like the email account, phone number, gender, and others. The user needs to consent the access to such fields.

Example: The user should have information of risk if the OSP request access to resources that it does not require to perform its functionalities (see full resources on Table 1).

User Story 3: Trust in the authentication system

As a user I want to be able to trust in the OSP using my email account, so that I can have guarantees that my data is kept private. My email provider needs to have a mechanism to verify the compliance of GDPR of OSP.

Note: My email provider (Gmail) and the OSP are different entities, and may take distinct approaches regarding GDPR compliance

Example: My email provider if fully compliant with GDPR, while the OSP is partially compliant with GDPR.

User Story 4: Proofs of GDPR compliance

As a service owner I want to be able to provide transparent proofs of GDPR compliance, so that users use my services. As a service I want to provide immutable proofs that I can comply with GDPR.

Note: I've been audited in terms of GDPR compliance, and I want to use proof of GDPR compliance to increase user trust on my service.

Example: The OSP was audited and certified in terms of GDPR compliance, such certification is held in a EVM blockchain.

User Story 5: No claims regarding GDPR compliance

As a service owner I want to provide my services, so that users can access with their email accounts to the provided functionalities without any concern of privacy management.

Note: This use story aims to exercise the different policies at the OpenID Provider.

Example: The OSP supports federation authentication, and it is up to the OpenID Provider (email service provider) to decide what to do upon non-proof of compliance.

Funded by the European Union

4 STATE OF THE ART ANALYSIS, BACKGROUND, AND INNOVATION

This section provides the background, the state of the art analysis and positions the innovations of OIDC PRINCE.

4.1 STATE OF THE ART ANALYSIS

This section provides an overview of the specifications/standards for OpenID Connect that support the functionalities of OIDC PRINCE. It provides an overview on Data Privacy vocabulary to express proofs of GDPR compliance, and available implementations that will support the OIDC PRINCE architecture.

▪ OpenID Connect Core

This section summarizes the information related with the OpenID connect protocols, considering the most relevant specifications [12] for this project, like the OpenID Connect Core [13].

The claims that are specified in the OpenID Core Specification are summarized in Table 1. OIDC also allows the specification of other claims, nonetheless, either the Relying Party (corresponding to OAuth 2.0 clients) and OpenID Provider (corresponding to the authorization servers in OAuth 2.0) need to support such claims.

The claims are different pieces of information or attributes about a user. Claims provide details about the user's identity.

TABLE 1 - OPENID CONNECT CORE SPECIFICATION CLAIMS

Member	**Type**	**Description**
sub	string	Subject - Identifier for the End-User at the Issuer.
name	string	End-User's full name in displayable form including all name parts, possibly including titles and suffixes.
given_name	string	Given name(s) or first name(s) of the End-User.
family_name	string	Surname(s) or last name(s) of the End-User.
middle_name	string	Middle name(s) of the End-User.
nickname	string	Casual name of the End-User that may differ of the given_name.
preferred_username	string	Shorthand name by which the End-User wishes to be referred to at the RP. This value MAY be a The RP MUST NOT rely upon this value being unique.

Funded by the European Union

		Values: ny valid JSON string including special characters such as @, /, or whitespace.
profile	string	URL of the End-User's profile page. The contents of this Web page SHOULD be about the End-User.
picture	string	URL of the End-User's profile picture.
website	string	URL of the End-User's Web page or blog. This Web page SHOULD contain information published by the End-User or an organization that the End-User is affiliated with.
email	string	End-User's preferred e-mail address. Its value MUST conform to the RFC 5322 addr-spec syntax.
email_verified	boolean	True if the End-User's e-mail address has been verified; otherwise false.
gender	string	End-User's gender. Values: female, male or others.
birthdate	string	End-User's birthday, ISO8601-1 YYYY-MM-DD format.
zoneinfo	string	String from IANA Time Zone For example, Europe/Paris or America/Los_Angeles.
locale	string	End-User's locale, represented as per RFC5646, which is is typically an ISO639 language code in lowercase and an ISO3166-1 country code in uppercase, separated by a dash. For example, en-US or fr-CA.
phone_number	string	End-User's preferred telephone number. E.164 is recommended as the format of this Claim, for example, +1 (425) 555-1212 or +56 (2) 687 2400.
phone_number_verified	boolean	True if the End-User's phone number has been verified; otherwise false.
address	JSON object	End-User's preferred postal address. The value of the address member is a JSON, as per RFC825
updated_at	number	Time the End-User's information was last updated. Its value is a JSON number representing the number of seconds from 1970-01-01T00:00:00Z as measured in UTC until the date/time.
claims_locales	String (optional)	To designate the loacle in IANA format. Example website#de to designate website in Germain.

The address claim includes the fields specified in Table 2.

TABLE 2 - OPENID CORE SPECIFICATION ADDRESS CLAIM

Member	**Type**	**Description**
formatted	string	Full mailing address
street_address	string	Street address number,
locality	string	City
region	string	State, province, region
postal_code		

Funded by the European Union

country	string	

The clients (Relying parties) can authenticate using the following methods:

- Client_secret_basic - Use a client_secret shared with the authorization server, and uses HTTP Basic Authentication scheme.
- Client_secret_post - Use a client_secret shared with the authorization server the client credentials are sent in the body.
- Client_secret_jwt - Use the client_secret and uses the HMAC SHA-256 and uses the JWT profile for authentication. The JWT contains divers information fields.
- Private_key_jwt - Client registers with a public key and signs a JWT with the public key.

Self-Issued OpenID Provider

This section summarizes the information related with the Self-Issued OpenID Providers V2 (SIOP) [14].

The SIOP specification extends OpenID Connect with the following aspects:

- Support for Decentralized Identifiers (DIDs) as Cryptographic Verifiable Identifiers
- Support for Cross-Device Self-Issued OP Model
- Support for non-registered RPs can pass data in metadata in the Authorization Request
- Support for Dynamic Self-Issued OpenID Provider Discovery
- Support for claimed URLs (universal links, app links), besides the custom URL
- Support to use any OpenID Connect flow for SIOPs and Dynamic Client Registration

Funded by the European Union

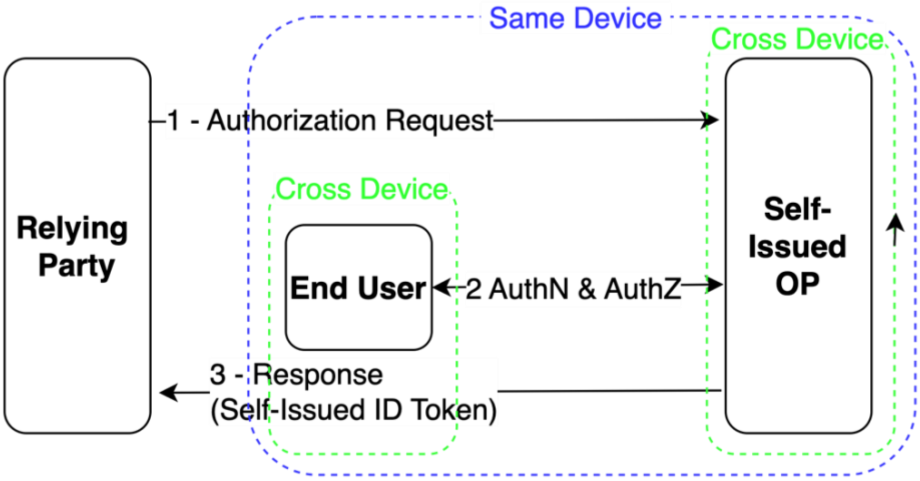


FIGURE 3 - SIOP FLOW WITH DIFFERENT MODELS

Figure 3 demonstrates the same and cross device models for the protocol flow:

- Same Device SIOP: SIOP is on the same device on which the interactions with the end-users occur. The trust provider can be a website on a different machine and uses the same SIOP protocol flow for authentication.
- Cross Device SIOP Self-issued OP in on a different device that the one on which the interactions with the End-User occur. In this model the communication between the RP and the SIOP cannot be processed through Redirects.

In the cross-device model the Relying Party users a QR code mechanism, that the user can scan on it's the mobile phone, where the SIOP is invoked with a customized URL and claimed URLs.

The SIOP is responsible to make available the required metadata in the endpoint */.well-known/openid-configuration*. This endpoint will contain all the information in a JSON format. The metadata of the SIOP can also be obtained from the *sub* claim. The metadata can include several information items [14] like scopes that are supported, signing algorithms for the ID tokens that are supported, the type of ID tokens that are supported. In this regard, SIOP adds the Self-Issued ID Token to OpenID Connect, that uses classical ID tokens [13].

▪ OpenID for Verifiable Presentations and Decentralized Identifiers

This section summarizes the information related with the OpenID for Verifiable Presentations [15]. OpenID for Verifiable Presentations works by enabling individuals to authenticate and share verifiable credentials with relying parties in a secure fashion.

The overall steps of Verifiable Presentations are:

1. **Issuer creates verifiable credentials**: A trusted entity, known as the issuer, creates verifiable credentials for individuals. These credentials contain claims about the individual, such as name, age.
2. **Presentation request from relying party**: When a user wants to access a service (relying party), the relying party sends a request for verifiable credentials. This request typically specifies the types of credentials required and any additional information needed.
3. **User authentication**: The user initiates authentication with their OpenID provider.
4. **Consent and authorization**: After authentication, the user is presented with a consent screen where they can review the information requested by the relying party and authorize the sharing of specific verifiable credentials.
5. **Verifiable presentation creation**: Once the user grants consent, the OpenID Connect provider constructs a verifiable presentation. This presentation includes the requested verifiable credentials along with cryptographic proofs to demonstrate their authenticity and integrity.
6. **Presentation to relying party:** The verifiable presentation is securely transmitted from the OpenID Connect provider to the relying party.
7. **Access granted**: Upon successful verification, the relying party grants the user access to the requested services or resources based on the information provided in the verifiable presentation.

Overall, OpenID for Verifiable Presentations enables individuals to assert their identity and share verified information with relying parties in a secure, privacy-preserving, and interoperable manner.

The DIDs can be used with Verifiable Credentials/Verifiable Presentations to support Self-Sovereign Identity (SSI) [16, 17]. DIDs work as digital identity management standard specified by W3C. DIDs provide a unique and persistent identifier for individuals, organizations, or things.

The verifiable presentations can reference DIDs as the subject of the presentation, ensuring that the credentials being presented are associated with a specific

Funded by the European Union

decentralized identity. Also, the verifiable credentials, which contain claims about an entity, can be linked to DIDs. These credentials are issued by trusted parties (issuers) and can include information such as a person's name, age, or qualifications. By associating verifiable credentials with DIDs, individuals can maintain control over their credentials and selectively disclose them as needed.

DIDs and verifiable credentials can be managed within decentralized identity wallets, that individuals use to store, manage, and present their digital identities and credentials. These wallets provide users with full control over their identities and credentials, enabling them to manage their digital interactions autonomously.

▪ Data Privacy Vocabulary and Extensions

The. W3C Data Privacy Vocabularies and Controls CG (DPVCG) develops a taxonomy of privacy and data protection related terms, refereed as Data Privacy Controls (DPV) [18]. DPV provides a taxonomy of personal data as well as a classification of purposes (i.e., purposes for data collection), and events of disclosures, consent, and processing such personal data.

The DPV specification [18] specifies the core components for the taxonomy of the personal data and its purposes. Allowing, as well the specification of extensions, which can include (not exhaustive list):

- Technology Concepts for DPV [20], that addresses the taxonomy to use to represent information related with technologies, such *SecurityTechnology*, *DataTechnology*, among others.
- Risk Assessment and Management Concepts for DPV [21] that addresses the taxonomy to use to represent information related with risk identification, assessment and management.
- EU-GDPR Extension for DPV [19] that addresses the aspects of providing proofs regarding the compliance of GDPR through DPV.

The DPV's terms are defined using RDF Schemas & Simple Knowledge Organization System (SKOS) semantics where all 'classes' and 'properties' are defined as *skos:Concept* in addition to *rdfs:Class* and *rdf:Property* respectively. For taxonomies or hierarchies, concepts are defined as 'instances' of a top-concept, and relationships within the hierarchy are defined using *skos:broader/skos:narrower*. For example, Purpose is the top concept within the taxonomy goals, and all purposes are instances of it.

The Web Ontology Language (OWL) is an alternate serialisation of DPV where the same concepts are defined using OWL semantics for use with OWL-based reasoners.

The core concepts in DPV include:

- PersonalData contains data directly or indirectly associated or related to an individual.
- Purpose specifies the goal of processing or using data or technology.
- Processing specifies the operations that can be performed on data.
- DataController specifies the individual or organisation that decides (or controls) the purpose(s) of processing personal data.
- DataSubject contains the individual (or category of individuals) whose personal data is being processed.
- LegalBasis is used to justify processing of data or use of technology in accordance with a law.
- Context provides relevant context information.

DPV also specifies the taxonomies for entities, purposes, processing, and others. Figure 4 exemplifies the entities of DPV.

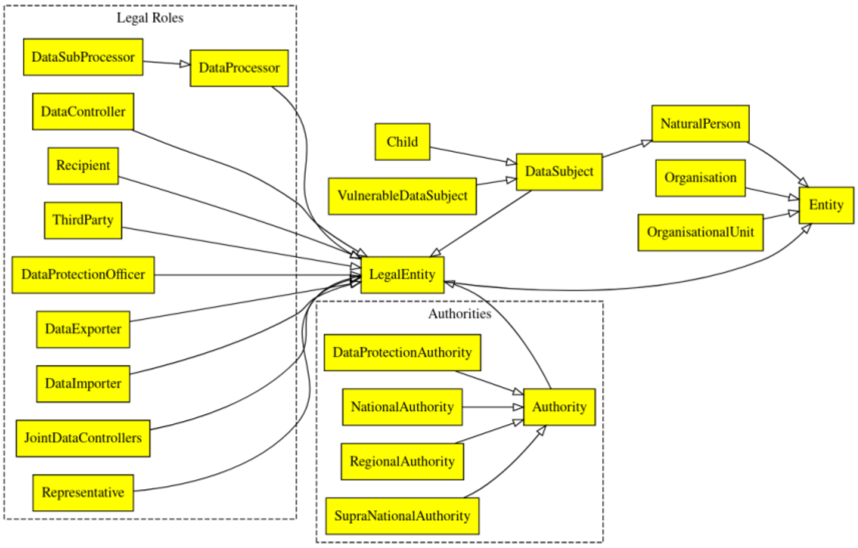


FIGURE 4 - ENTITIES IN DPV (SOURCE [19])

EU-GDPR Extension for DPV [19] allows to express the compliance level in three classes:

- GDPR Compliance Unknown – not known the GDPR compliance
- GDPR Compliant - State of being lawful or legally compliant for GDPR

- GDPR Lawfulness - Status or state associated with being lawful or legally compliant regarding GDPR
- GDPR Non-compliant - State of being unlawful or legally non-compliant for GDPR

The following DPV example illustrates the indication that the personal data is sensitive.

```
ex:PatientStudy rdf:type dpv:PersonalDataHandling ;
    dpv:hasPersonalData ex:BloodSamples, ex:PatientIdentifier .

ex:BloodSamples rdf:type dpv:SpecialCategoryPersonalData ;
    skos:broader dpv-pd:MedicalHealth ;
    skos:narrower dpv-pd:BloodType .

ex:PatientIdentifier rdf:type dpv:SensitivePersonalData ;
skos:broader dpv-pd:Identifying .
```

This example also illustrates the information of compliance for *serviceA* using the EU GDPR extension.

```
ex:ServiceA rdf:type dpv:Service ;
   eu-gdpr:GDPRLawfulness eu-gdpr:GDPRCompliant.
```

▪ Open-Source Solutions for OpenID Connect Support

This section summarizes the open-source solutions that are relevant for the choice of tools to build OIDC-PRINCE.

Table 3 lists the solutions that were surveyed in terms of enabling a OpenID Provider, and their support towards SSI paradigm (SIOP and VC/VP).

TABLE 3 - OPEN-SOURCE SOLUTIONS WITH SUPPORT FOR OPENID CONNECT

Solution	Purpose and Description	Advantages	License
Ory Kratos (github)	Identity and User management system	Cloud-Native (runs on Kubernetes) Supports MutiFactor Authentication	Apache 2.0
Ory Hydra (github)	OpenID OAuth 2 and OpenID Connect Provider	**OpenID Certified** Can be used with different identity solutions (Ory Kratos, authboss, User Frosting)	Apache 2.0
Agama OpenID Connect Project (github)			
Janssen Project (github)	Open-source digital identity platform	Integrates with Keycloak Has a certified OpenID Connect Provider Has differente deployment options Has a commercial version (Gluu Server)	Apache 2.0
Keycloak [1](github)	Open-Source Identity and Access Management solution	With: - FAPI 2 draft support - Demonstration Proof-of-Possession (DPoP) Authentication with PassKeys Has a plugin to support SIOP https://github.com/FIWARE/keycloak-vc-issuer	Apache 2.0
Shepereon[2] (github)	Self-Issued OpenID Provider (SIOPv2) with OpenID4VP support	Seems to fully support SIOP and OID4VC. Has the drawback of being in development phase	Apache 2.0

Keycloak is an Open Source Identity and Access Management that provides single sign on solution (SSO) for web apps and RESTful web services [22]. The goal of Keycloak is to make security simple so that it is easy for application developers to secure the apps and services they have deployed in the organizations.

Some of the features offered by Keycloak include Roles and subgroups, Central administrator management, Impersonation, Advanced password policy, Plugin-based architecture.

KeyCloak is a featured project inside the cloud native computing foundation and is also used by industry and big players, like CERN as the IAM solution [23]. Keycloak does not yet support SIOP, there are some proof of concepts that can be enabled to support

[1] Feasible solution as being a reference implementation of Identity Management

[2] Feasible solution as being a solution that implements SIOP.

Funded by the European Union

SIOPv3 and OIDC4VC, as per the Keycloak community design documentation [24].

The Sphereon SIOP-OID4VP is a project from the NGI Ontochain project that implements SIOP and OID4VP. The source code is available on github [25] and follows the following recommendations:

- SIOPv2 specification version discovery with support for the latest development version (draft 11), Implementers Draft 1 and the JWT VC Presentation Interop Profile.
- Verifiable Presentation and Presentation Exchange support on the RP and OP sides, according to the OpenID for Verifiable Presentations (OID4VP) and Presentation Exchange specifications.

Nonetheless this project is still in active development.

Open-Source Solutions for Use Cases Support

This section summarizes the open-source solutions that are relevant for the choice of tools to validate the OIDC-PRINCE framework in the validation of the use cases: Education and online selling platform.

It was established a requirement of these tools to already support OpenID Connect or OAuth, otherwise they cannot be employed to evaluate the use cases.

TABLE 4 - OPEN-SOURCE SOLUTIONS FOR EDUCATION USE CASE

Solution	Purpose and Description	Advantages / Disadvantages	License
Moodle with OpenID Connect Authentication Plugin (moodle.org) (github.com)	Enable SSO functionality in Moodle. It connects with Azure Active Directory, but can also support for OpenID Connect providers	Moodle is a established platform in Open Source community as a Learning Management Platform	GNU Public License v3 (License)
Sakai (github.com)	Collaboration and Learning Environment	Can use external tools to handle the authentication and authorization through OAuth and OpenID Connect.	Educational Community License v2.0 (License)
Open edX (github.com)	Source code, powering the platform edX.	Supports OAuth2.0 and OpenID Connect but for specific (E-commerce service)	GNU Affero General Public License v3.0 (License)

The choice relies on Moodle, mainly due its higher customization and our knowledge on the Moodle platform at courses in the university.

TABLE 5 - OPEN SOURCE SOLUTION FOR ONLINE SELLING PLATFORM

Solution	Purpose and Description	Advantages	License
eBay with OpenID Connect Authentication Plugin (ebay.com) (github.com)	->Improve the authentication mechanism on the platform, providing a more secure, standardized and user-friendly way for users. ->The OIDC authentication plug-in adds an additional layer to eBay's authentication process.	-> Secure authentication. -> Easy integration. ->Current security standards. ->Single Sign-On (SSO). ->ID Token.	Apache License 2.0 (License)
WooCommerce WorPress plugin [26]	->Implementing OpenID Connect with WooCommerce server to enhance both the security and the user experience for our online store.	->SSO ->Enhanced Security ->Trusted Identity Providers ->Scalability and Flexibility ->Compliance with Standards: OpenID Connect is a widely adopted standard, ensuring compatibility and interoperability	GPLv2 or later (License)

The WooCommerce was chosen since it is a WordPress plugin that supports OpenID Connect authentication (video).

▪ State of the Art - Scientific manuscripts

This section summarizes the state of the art in term of scientific manuscripts published in conferences and journals.

Holtmann [27] performed an analysis of the implementation of OIDC and the security elements that enable SSO. The purpose of their work was to perform a vulnerability assessment.

As OIDC is one of the solutions that enable SSO for Web applications, authors such as Naik et al. [28] perform an evaluation of SAML, OAuth 2.0, and OIDC on the security strength. The work of Naik et al. complements the work of Holtmann on the vulnerability assessment of OIDC.

On the same line, the RAD-AA framework determines the risk of based authentication and authorization approaches, comparing the OAuth2, SAML and OpenID Connect protocols [29]. The work is mainly devoted to evaluating ML models to determine the risk associated with such protocols.

Other works like Jorge et al. [30], Fritsch et al. [31], Sassetti et al. [32], Li et al. [33] mainly analyse the privacy support in OpenID Connect, OAuth2 and how they can be mitigated. The work of Carsten [34] employ Multiparty computation (MPC) and zero proof knowledge to enhance privacy support. The employment of such techniques greatly contributes to enhance support privacy, but do not solve the issues in OpenID consents, which do not provide information to the user regarding privacy risks or the trustworthiness of services, with which the user is interacting and sharing data.

The work of Belfaik et al. [42] adds more security to OIDC by proposing the use of blockchain to protect several parameters like *client_id, client_secret, authorization code, access token, id token, state,* and *redirect_uri*, as these can led to security and privacy issues.

D^2-IAM is proposed by Somchart et al. [43] to enable efficient support for SSO in multi-applications and multi-user environments. The proposal relies on blockchain and enables policies support for each user, nonetheless it mainly targets cloud scenarios.

To the best of our knowledge no approach has yet, combined data privacy techniques with OpenID Connect in a standard fashion and leveraging on decentralized identifiers and verifiable proofs.

4.2 DESCRIPTION OF BACKGROUND

We will be using, mainly our knowledge in the OIDC PRINCE. This knowledge is in two domains:

- **Authentication, Authorization through OpenID Connect domain**. OIDC has been employed to introduce new functionalities like the OIDC-TCI [3], which enables the enforcement of authentication policies considering the context information. This work has considered in securing devices in IoT use cases [2] and securing the authentication and authorization in Software Defined Networks (SDN) [1]. Most of these solutions have relied on Keycloak as the OpenID Connect Provider solution.
- **Privacy and Risk Management domain**, using diverse approaches like Fuzzy Models, Natural Language Processing (NLP) for privacy-preserving solutions [4-5], or to detect violations in online contracts [6]. The fuzzy models will be relevant to determine the risk associated with the consents.

Funded by the European Union

4.3 INNOVATION COMPARED TO THE STATE OF THE ART

The innovations of OIDC PRINCE are associated with the that are associated with planned functionalities and are as follows:

- **Inov. 1 Integrated solution for trust enhancement in SSO**: The OIDC PRINCE framework integrates the current standards on identity management (DIDs) and verifiable credentials/presentations into SSO, using DPV that convey information regarding GDPR compliance. This will contribute towards trustworthy solutions and will contribute towards a faster adoption of digital identity management solutions like SSI into authentication and authorization processes.

  This innovation is related with the following functionalities:

  1. Manage documents proving GDPR compliance (DPV)
  2. Manage identity of services in a decentralized fashion (DIDs)

- **Inov. 2 Risk analysis considering the resources/claims that are requested in consent operations**: The risk analysis relies on fuzzy models, that consider the type of service requesting access, the requested claims, and the GDPR compliance levels to provider user the privacy risks that might be associated the consent. For instance, what risks might be associated by the sharing of mobile phone with a service, that does not need such information to provide its functionalities.

  This innovation is related with the following functionality:

  1. Risks analysis in consents (Fuzzy Models)

- **Inov. 3 Policies for SSO operations according to the levels of GDPR compliance:** The fact of having GDPR compliance information allows OpenID Connect Providers to harden the security and trust of the OpenID ecosystem. Relying parties (clients) providing proofs of the GDPR compliance can be considered trustworthy and thus be accepted without any restriction on the client registration. On the other hand, clients with partial or no GDPR compliance, are prone to more restrictive policies on the side of OpenID connect providers, that can even not accept such type of clients. Of, if accepted on the registration, restrict the information that they can have access.

  This innovation is related with the following functionality:

  1. Policies management as per GDPR compliance levels by OpenID Provider

5 SOFTWARE DESIGN AND ANALYSIS, COMPONENT SPECIFICATION (PRELIMINARY)

This section presents the architecture of OIDCE PRINCE. The architecture of OIDC-Prince is depicted in Figure 5.

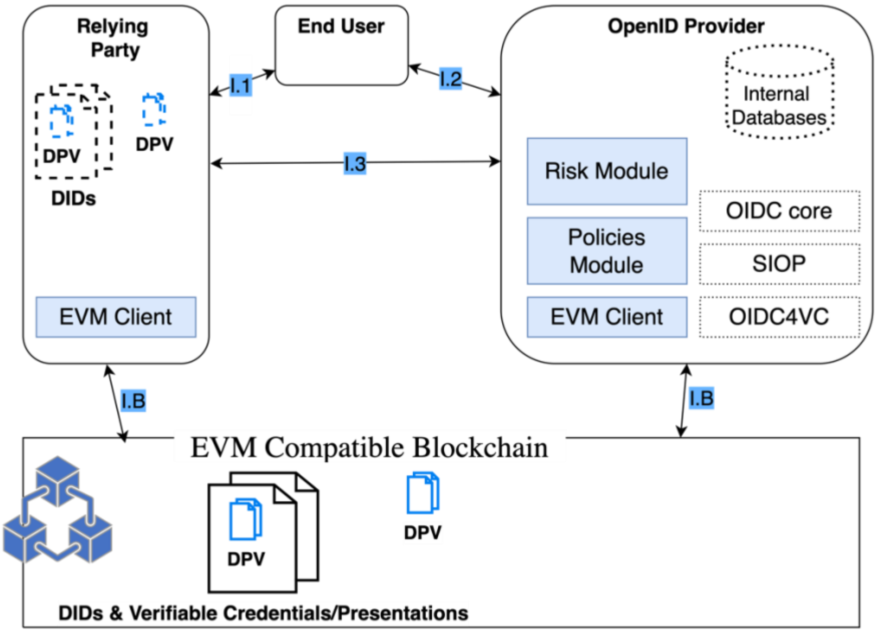


FIGURE 5 – PRELIMINARY OIDC PRINCE ARCHITECTURE AND INTERFACES

The modules/components to be developed in OIDC-Prince are:

- **Risk Module** – this component has the goal to determine the risk associated with the different authentication and authorization processes.
- **Policy Module** – this component is used to perform policies enforcement in the authentication and authorization flows, according to the GDPR compliance level.
- **EVM Client** – this component makes the interface with the EVM blockchain to manage data (CRUD operations).

Funded by the European Union

The main interfaces in the OIDC-Prince architecture are:

- I.1 – standard OIDC interface, for authorization flow,
- I.2 – OIDC interface but with information of risk regarding a particular flow/process, with the identification of the user (DID). Through this interface is exchanged the following information:
    - Identification of user
    - Result of the risk analysis regarding the requested processes/flows.
- I.3 – OIDC interface with information of the relying party (DIDs) and requested claims. Through this interface it is communicated the following information:
    - Identification of service
    - Identification of requested claims
    - Address/identity used in blockchain to be verified the compliance of the service
- I.B – interface used by the EVM client to manage DPVs in the EVM blockchain.
    - CRUD of DPVs
    - CRUD of DIDs

5.1 SOFTWARE MODULES

The modules to be developed in the context of the TRUSTCHAIN open call include the risk module, the policy module both running at the OpenID Connect Provider and the EVM Client, which will be required at the relying party and at the OpenID Connect Provider.

▪ Risk Module

The Risk Module component has the goal to determine the risk associated with the different authentication and authorization processes. To determine the risk this component uses Fuzzy Models to assess the risk associated with the access authorization to claims (when requested by service that can or cannot be compliant with GDPR).

This component using the Fuzzy Models will consider the following details:

- Type of service – if it is service for education, for online selling, or others.

- Set of requested claims – the requested claims, which access was required.
- Proofs of GDPR compliance - the DPV-based proofs of GDPR compliance
- Time of registration in OpenID Connect Provider
- Previous iterations with the OpenID Provider

Before being fully integrated with the OIDC PRINCE framework, initial validation of the fuzzy models will be performed using tools like Fuzzy Logic SciKit (for Python SciPy) [35]. These fuzzy models will be integrated into Keycloak to operate on the authorization flows of OpenID Connect.

Policy Module

The Policy Module component is used to perform policies enforcement in the authentication and authorization flows, according to the GDPR compliance level.

The policies will be developed in the Keycloak using different policies like [36]:

- JavaScript-based policy to specify policies regarding the access management of objects.
- Client-based policy that allow to define conditions that clients (relying parties) need to meet to access objects.
- Aggregated policies that allow the aggregation of different types of policies to provide a final decision regarding the access to objects.

Keycloak already includes a Policy Enforcement Point (PEP) as demonstrated in Figure 6. This policy module will specify the policies for the PEP enforcement actions.

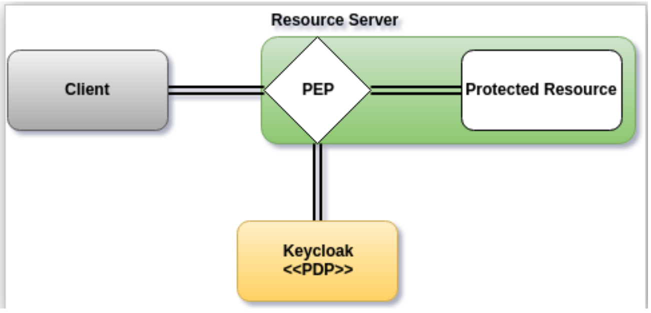


FIGURE 6 - POLICY ENFORCEMENT POINT IN KEYCLOAK (SOURCE [37])

Funded by the European Union

▪ EVM Client

The EVM Client component makes the interface with the EVM blockchain to manage data (CRUD operations). This component is responsible to DPV, DIDs in the EVM blockchain. It is worth mentioning that this component exists in the Relying Party and on the Authorization Server/Identity Provider server. On the side of the relying party the, the EVM client enables the upload of DPV compliance proofs in the EVM blockchain, according to the identification of the service (DIDs).

It should be noted that two versions of the EVM client will be produced:

- A version for the relying party
- A version for the OIDC provider, which aims to be integrated into Keycloak.

5.2 WORK PLAN FOR DEPLOYMENT

Figure 7 depicts all modules that will be developed and used in OIDC PRINCE. In blue are all the modules that will be developed in OIDC PRINCE. The white ones will be used from the existing solutions.

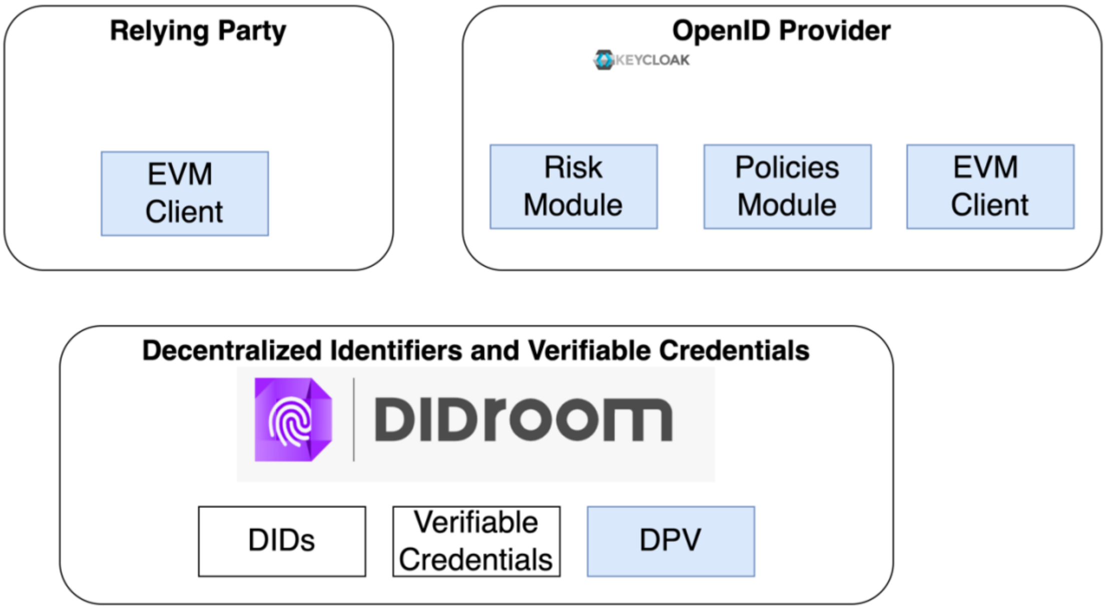


FIGURE 7 – DEPLOYMENT PLAN FOR MODULES OF OIDC PRINCE (BLUE WILL BE DEVELOPED IN OIDC)

Funded by the European Union

The detailed plan includes the following:

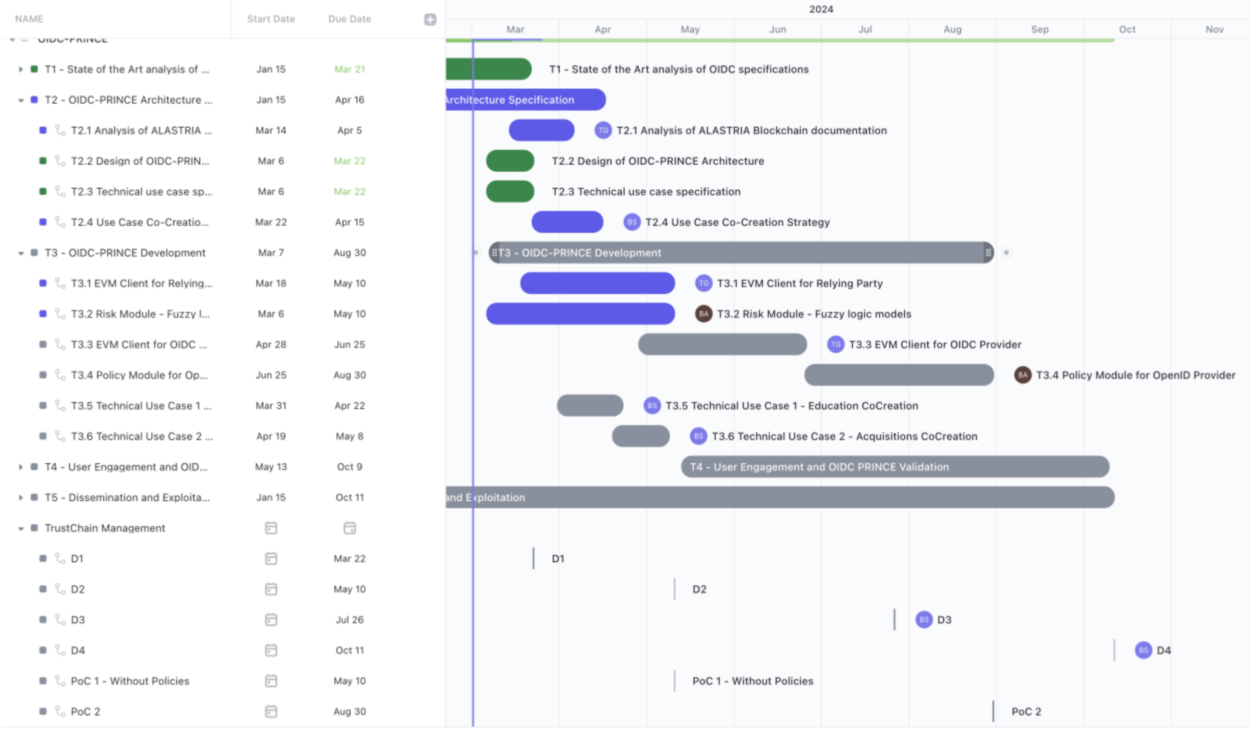
- DID and Verifiable Credentials Solutions from ForkBOMB [39], one of the OC1 TRUSTCHAIN projects. The DIDroom solution will used to enable the support of DIDs and VCs.
- DPV will be implemented in the project. In particular the DIDroom solution [39] will be used to extended the information of GDPR compliance.
- The EVM client at the relying party will be developed in Python relying on the module py-em [38] and will have APIs to interact with Moodle OIDC plugin and with the Woocommerce.
- The risk module will be validated with tools like Fuzzy Logic SciKit (for Python SciPy) [35] and integrated in Keycloak using plugins/extensions [40, 41]. The risk module will be implemented using Java technology on Keycloak.
- The policies module, as stated, will be implemented using the facilities in Keycloak for policy management [36] and enforced with the existing PEP [37]. The development will mainly rely on JavaScript language to allow the specification of complex policies.

6 DETAILED WORK PLAN FOR IMPLEMENTATION AND DEPLOYMENT (PRELIMINARY)

The teams is composed mainly by:

- Bruno Sousa (BS), an assistant professor at the University of Coimbra, with expertise on OpenID Connect
- Bernardo Arzileiro (BA), a master student at the Master on Engineering Informatics
- Tiago Galvão (TG), a master student at the Master on Security Informatics
- Paulo Silva (PS), a senior researcher at CISUC, and with expertise on data privacy.

The overall Gantt diagrams is pictured in Figure 8.



NAME	Start Date	Due Date
OIDC-PRINCE		
T1 - State of the Art analysis of ...	Jan 15	Mar 21
T2 - OIDC-PRINCE Architecture ...	Jan 15	Apr 16
T2.1 Analysis of ALASTRIA ...	Mar 14	Apr 5
T2.2 Design of OIDC-PRIN...	Mar 6	Mar 22
T2.3 Technical use case sp...	Mar 6	Mar 22
T2.4 Use Case Co-Creatio...	Mar 22	Apr 15
T3 - OIDC-PRINCE Development	Mar 7	Aug 30
T3.1 EVM Client for Relying...	Mar 18	May 10
T3.2 Risk Module - Fuzzy l...	Mar 6	May 10
T3.3 EVM Client for OIDC ...	Apr 28	Jun 25
T3.4 Policy Module for Op...	Jun 25	Aug 30
T3.5 Technical Use Case 1 ...	Mar 31	Apr 22
T3.6 Technical Use Case 2 ...	Apr 19	May 8
T4 - User Engagement and OID...	May 13	Oct 9
T5 - Dissemination and Exploita...	Jan 15	Oct 11
TrustChain Management		
D1		Mar 22
D2		May 10
D3		Jul 26
D4		Oct 11
PoC 1 - Without Policies		May 10
PoC 2		Aug 30

2024
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
T1 - State of the Art analysis of OIDC specifications
Architecture Specification
T2.1 Analysis of ALASTRIA Blockchain documentation
T2.2 Design of OIDC-PRINCE Architecture
T2.3 Technical use case specification
T2.4 Use Case Co-Creation Strategy
T3 - OIDC-PRINCE Development
T3.1 EVM Client for Relying Party
T3.2 Risk Module - Fuzzy logic models
T3.3 EVM Client for OIDC Provider
T3.4 Policy Module for OpenID Provider
T3.5 Technical Use Case 1 - Education CoCreation
T3.6 Technical Use Case 2 - Acquisitions CoCreation
T4 - User Engagement and OIDC PRINCE Validation
and Exploitation
D1
D2
D3
D4
PoC 1 - Without Policies
PoC 2

FIGURE 8 - GANTT DIAGRAM

The overall tasks of the project plan are presented in Figure 9. With the writing of this document T1 with the state-of-the-art analysis is concluded. T2 with the specification of the preliminary architecture, which will be refined in T3, is partially implemented (50%).

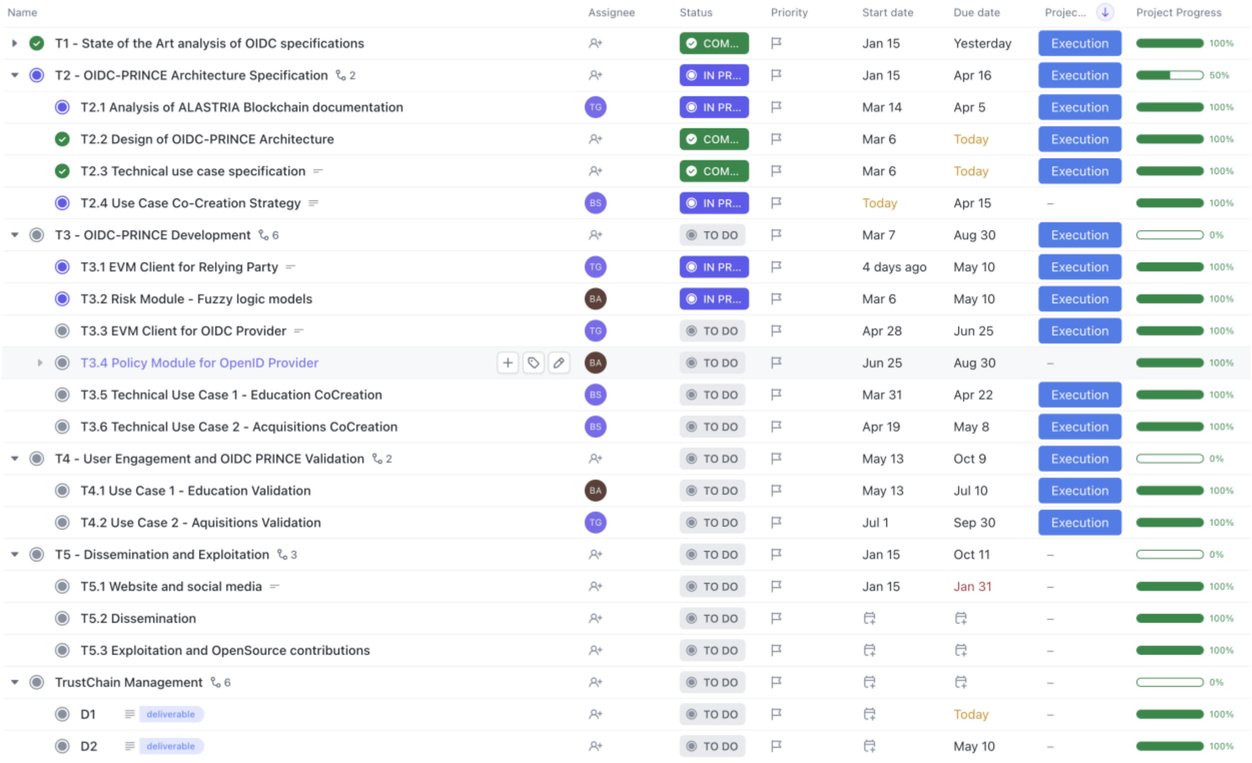
T3 is dedicated to the development of the modules:

- T3.1 – EVM client for relying party
- T3.2 – Risk Module with fuzzy logic models
- T3.3 – EVM client for OIDC Provider
- T3.4 – Policy Module for OIDC Provider

T4 is related user engagement for use cases evaluation.

The project has planned two proofs of concepts:

- PoC 1 – in May/24, this is to allow the start of the user evaluation activities in T4
- Poc 2 – in August/24, this PoC includes policies support in the OpenID Connect Provider, namely in Keycloak.



Name	Assignee	Status	Priority	Start date	Due date	Projec...	Project Progress
T1 - State of the Art analysis of OIDC specifications		COM...		Jan 15	Yesterday	Execution	100%
T2 - OIDC-PRINCE Architecture Specification 2		IN PR...		Jan 15	Apr 16	Execution	50%
T2.1 Analysis of ALASTRIA Blockchain documentation	TG	IN PR...		Mar 14	Apr 5	Execution	100%
T2.2 Design of OIDC-PRINCE Architecture		COM...		Mar 6	Today	Execution	100%
T2.3 Technical use case specification		COM...		Mar 6	Today	Execution	100%
T2.4 Use Case Co-Creation Strategy	BS	IN PR...		Today	Apr 15	–	100%
T3 - OIDC-PRINCE Development 6		TO DO		Mar 7	Aug 30	Execution	0%
T3.1 EVM Client for Relying Party	TG	IN PR...		4 days ago	May 10	Execution	100%
T3.2 Risk Module - Fuzzy logic models	BA	IN PR...		Mar 6	May 10	Execution	100%
T3.3 EVM Client for OIDC Provider	TG	TO DO		Apr 28	Jun 25	Execution	100%
T3.4 Policy Module for OpenID Provider	BA	TO DO		Jun 25	Aug 30	–	100%
T3.5 Technical Use Case 1 - Education CoCreation	BS	TO DO		Mar 31	Apr 22	Execution	100%
T3.6 Technical Use Case 2 - Acquisitions CoCreation	BS	TO DO		Apr 19	May 8	Execution	100%
T4 - User Engagement and OIDC PRINCE Validation 2		TO DO		May 13	Oct 9	Execution	0%
T4.1 Use Case 1 - Education Validation	BA	TO DO		May 13	Jul 10	Execution	100%
T4.2 Use Case 2 - Aquisitions Validation	TG	TO DO		Jul 1	Sep 30	Execution	100%
T5 - Dissemination and Exploitation 3		TO DO		Jan 15	Oct 11	–	0%
T5.1 Website and social media		TO DO		Jan 15	Jan 31	–	100%
T5.2 Dissemination		TO DO				–	100%
T5.3 Exploitation and OpenSource contributions		TO DO				–	100%
TrustChain Management 6		TO DO				–	0%
D1 deliverable		TO DO			Today	–	100%
D2 deliverable		TO DO			May 10	–	100%

FIGURE 9 - PROJECT PLAN

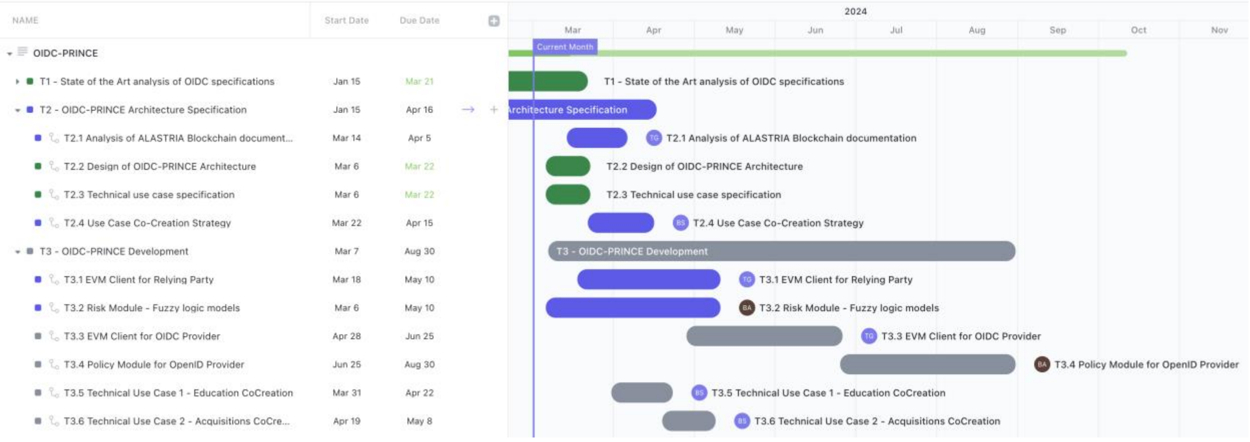
6.1 WORK PLAN FOR IMPLEMENTATION

The implementation if mainly performed in T2 and T3, with the following subtasks:

- T2.1 – Analysis of Alastria blockchain – gathering knowledge of the APIs, required keys to publish data in the EVM blockchain. Subtask performed by Tiago.
- T3.1 – EVM client for relying party – this subtask aims to develop the EVM client that can be used in the technical solutions chosen for the use cases. In the education, the EVM client will interact with Moodle OIDC plugin, to convey the information in the EVM blockchain. In the OSP use case, the woocomerce plugin will be modified to interact with the EVM client. Subtask performed by Tiago.
- T3.2 – Risk Module with fuzzy logic models this subtask leads to the implementation of the fuzzy models in the risk module. Subtask performed by Bernardo and Paulo.

- T3.3 – EVM client for OIDC Provider, as the OIDC Provider uses different technologies, a specific client will be built in the Keycloak in the form of plugins. Subtask performed by Tiago.
- T3.4 – Policy Module for OIDC Provider the policy module will be built after the first PoC, as this functionality does not involve the end-user. Subtask performed by Bernardo and Bruno.

Figure 10 details the overall Gantt diagram for the implementation tasks.



NAME	Start Date	Due Date
OIDC-PRINCE		
T1 - State of the Art analysis of OIDC specifications	Jan 15	Mar 21
T2 - OIDC-PRINCE Architecture Specification	Jan 15	Apr 16
T2.1 Analysis of ALASTRIA Blockchain document...	Mar 14	Apr 5
T2.2 Design of OIDC-PRINCE Architecture	Mar 6	Mar 22
T2.3 Technical use case specification	Mar 6	Mar 22
T2.4 Use Case Co-Creation Strategy	Mar 22	Apr 15
T3 - OIDC-PRINCE Development	Mar 7	Aug 30
T3.1 EVM Client for Relying Party	Mar 18	May 10
T3.2 Risk Module - Fuzzy logic models	Mar 6	May 10
T3.3 EVM Client for OIDC Provider	Apr 28	Jun 25
T3.4 Policy Module for OpenID Provider	Jun 25	Aug 30
T3.5 Technical Use Case 1 - Education CoCreation	Mar 31	Apr 22
T3.6 Technical Use Case 2 - Acquisitions CoCre...	Apr 19	May 8

2024
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Current Month
T1 - State of the Art analysis of OIDC specifications
rchitecture Specification
TG T2.1 Analysis of ALASTRIA Blockchain documentation
T2.2 Design of OIDC-PRINCE Architecture
T2.3 Technical use case specification
BS T2.4 Use Case Co-Creation Strategy
T3 - OIDC-PRINCE Development
TG T3.1 EVM Client for Relying Party
BA T3.2 Risk Module - Fuzzy logic models
TG T3.3 EVM Client for OIDC Provider
BA T3.4 Policy Module for OpenID Provider
BS T3.5 Technical Use Case 1 - Education CoCreation
BS T3.6 Technical Use Case 2 - Acquisitions CoCreation

FIGURE 10 - GANTT DIAGRAM FOR T3 TASK

6.2 WORK PLAN FOR DEPLOYMENT

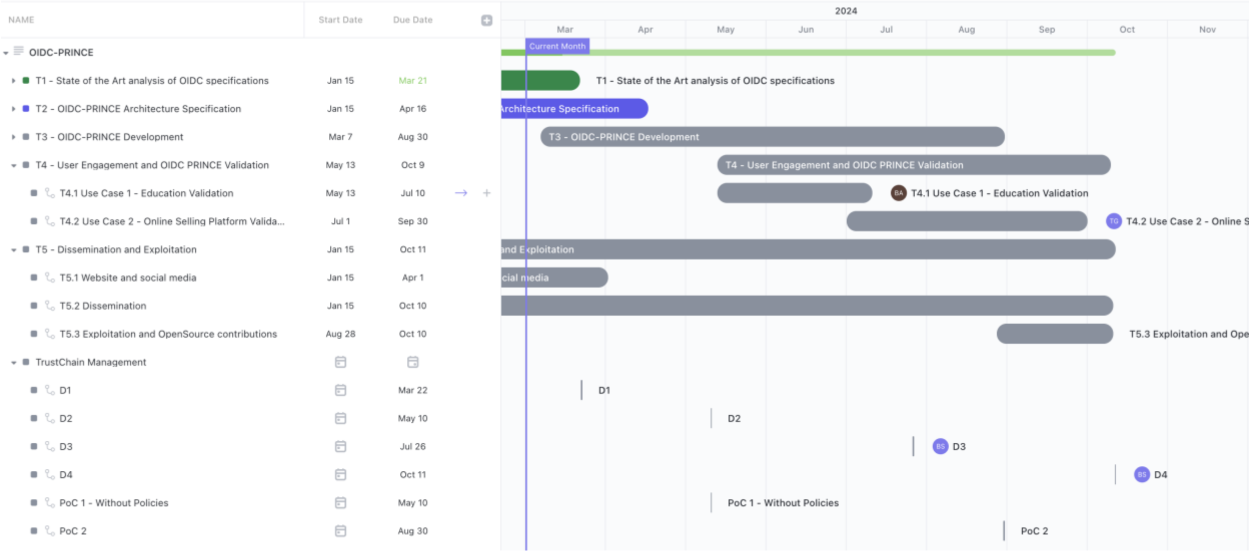
The deployment mainly involves tasks T4 and T5, with the following subtasks:

- T4.1 – Use case 1 – Education validation, this will be the first case to be validated, and will serve to validate the cocreation strategy for this use case and to correct, enhanced modules according to the received feedback. Subtask with the participation of all the team, but with a major effort from Bernardo.
- T4.2 – Use case 2 – Online Selling Platform validation the last use case will include the policies functionality and will start by having integrated the required modifications. The user cocreation will rely on the same volunteers of use case 1. Subtask with the participation of all the team, but with a major effort from Tiago.
- T5.1 – website and social media, a draft site was already created and is available at: https://oidc-prince.github.io/oidc-prince-site/. The website will be updated with the funding information from Trustchain and with the placeholders for

news and achievements throughout the project lifetime. Subtask with the participation of all the team, but with a major effort from Bruno.

- T5.2 – Dissemination this task is related with the dissemination of the project, which will have information aggregated at the web site and will include the dissemination of the work in scientific venues and journals. A preliminary target list of possible venues for dissemination includes:
  - ACM Transaction on Privacy and Security (ISSN: 2471-2566)
  - IEEE/IFIP Network Operations and Management Symposium (IEEE IM/NOMS)
  - IEEE International Conference on Computer Communications (IEEE Infocom)
- T5.3 – Exploitation and OpenSource Contributions this subtask is mainly devoted to the release of opensource contributions in the repositories of the TRUSTCHAIN and on the official repository of the project:
  - https://github.com/NGI-TRUSTCHAIN/OIDC-PRINCE -- Repository in the TRUSTCHAIN project
  - https://github.com/OIDC-PRINCE/oidc-prince -- Oficial repository of the project, that at the time of this deliverable is still private. Will be made public in the context of this task and after PoC 2.

Figure 11 shows the detailed Gantt diagram for these two tasks.



NAME	Start Date	Due Date
OIDC-PRINCE		
T1 - State of the Art analysis of OIDC specifications	Jan 15	Mar 21
T2 - OIDC-PRINCE Architecture Specification	Jan 15	Apr 16
T3 - OIDC-PRINCE Development	Mar 7	Aug 30
T4 - User Engagement and OIDC PRINCE Validation	May 13	Oct 9
T4.1 Use Case 1 - Education Validation	May 13	Jul 10
T4.2 Use Case 2 - Online Selling Platform Valida...	Jul 1	Sep 30
T5 - Dissemination and Exploitation	Jan 15	Oct 11
T5.1 Website and social media	Jan 15	Apr 1
T5.2 Dissemination	Jan 15	Oct 10
T5.3 Exploitation and OpenSource contributions	Aug 28	Oct 10
TrustChain Management		
D1		Mar 22
D2		May 10
D3		Jul 26
D4		Oct 11
PoC 1 - Without Policies		May 10
PoC 2		Aug 30

2024
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Current Month
T1 - State of the Art analysis of OIDC specifications
rchitecture Specification
T3 - OIDC-PRINCE Development
T4 - User Engagement and OIDC PRINCE Validation
BA
T4.1 Use Case 1 - Education Validation
TG
T4.2 Use Case 2 - Online S
nd Exploitation
cial media
T5.3 Exploitation and Ope
D1
D2
BS
D3
BS
D4
PoC 1 - Without Policies
PoC 2

FIGURE 11 - GANTT DIAGRAM FOR T4 AND T5 TASKS

Funded by the European Union

7 CONCLUSIONS

OIDC PRINCE envisions to enhance the privacy support in user consents used in OpenID Connect authentication and authorization processes. As users need to be informed regarding the potential risk of providing consent for the personal information access by services/entities that may not be trusted by the user and the OpenID Provider, which is responsible to manage the authentication and authorization.

This document documents the functionalities of OIDC PRINCE towards its major goal and details the plan for the deployment and implementation of functionalities. The OIDC PRINCE team has a multidisciplinary team, with different expertise areas including privacy, risk management and authentication.

The document also drafts a preliminary architecture of OIDC PRINCE, where the main modules of OIDC PRINCE are identified, including the Risk module, the Policy Module and the EVM Client.

REFERENCES

[1] Bruno Sousa, Carolina Gonçalves, FedAAA-SDN: Federated Authentication, Authorization and Accounting in SDN controllers, Computer Networks, Volume 239, 2024, 110130, ISSN 1389-1286, DOI

[2] C. Gonçalves, Bruno Sousa, M. Vukovic and M. Kusek, A federated authentication and authorization approach for IoT farming, in Internet of Things, 2023, DOI

[3] C. Gonçalves, Bruno Sousa and N. Antunes, OIDC-TCI: OIDC with Trust Context Information, in IFIP Wireless and Mobile Networking Conference (WMNC), 2022 DOI

[4] C. Gonçalves, N. Antunes, M. Curado, P. G. Silva and B. Walek, Privacy risk assessment and privacy-preserving data monitoring, Expert Systems with Applications, in Expert Systems with Applications, vol. 200, no. 116867, 2022, DOI

[5] M. Cunha, R. Mendes and J. P. Vilela, A survey of privacy-preserving mechanisms for heterogeneous data types, Computer Science Review, vol. 41, 2021, DOI

[6] P. G. Silva, C. Godinho, C. Gonçalves, N. Antunes and M. Curado, Using Natural Language Processing to Detect Privacy Violations in Online Contracts, in The 35th ACM/SIGAPP Symposium on AppliedComputing (SAC '20), 2020, DOI

[7] Navas, Jorge, and Marta Beltrán. "Understanding and mitigating OpenID Connect threats." Computers & Security 84 (2019): 1-16, DOI.

[8] Li, Wanpeng, and Chris J. Mitchell. "User access privacy in OAuth 2.0 and OpenID connect." In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 664-6732. IEEE, 2020, DOI

[9] Sven Hammann, Ralf Sasse, and David Basin. 2020. Privacy-Preserving OpenID Connect. In Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20). Association for Computing Machinery, New York, NY, USA, 277–289, DOI

[10] J. Primbs and M. Menth, "OIDC2: Open Identity Certification With OpenID Connect," in IEEE Open Journal of the Communications Society, doi: 10.1109/OJCOMS.2024.3376193. DOI

[11] European Digital Identity, available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

[12] OpenID Specifications, available at: https://openid.net/developers/specs/

[13] OpenID Connect Core 1.0, available at: https://openid.net/specs/openid-connect-core-1_0.html

[14] Self-Issued OpenID Provider, available at: https://openid.net/specs/openid-connect-self-issued-v2-1_0.html

[15] OpenID for Verifiable Presentations, available at: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html

[16] S. Huh, M. Shim, J. Lee, S. S. Woo, H. Kim and H. Lee, "DID We Miss Anything?: Towards Privacy-Preserving Decentralized ID Architecture," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 6, pp. 4881-4898, Nov.-Dec. 2023, DOI

[17] W3C, "Decentralized Identifiers (DIDs)",2022, https://www.w3.org/TR/did-core/

[18] W3C, “Data Privacy Vocabulary (DPV)”, 2024, https://w3c.github.io/dpv/dpv/

[19] W3C, “EU-GDPR Extension Data Privacy Vocabulary”, 2023, https://w3c.github.io/dpv/legal/eu/gdpr/

[20] W3C, “Technology Concepts for DPV”, https://w3c.github.io/dpv/tech/

Funded by the European Union

[21] W3C, Risk Extension for DPV, https://w3c.github.io/dpv/risk/

[22] Keycloak, available at: https://www.keycloak.org/

[23] CERN Authorization Servicer, available at: https://auth.docs.cern.ch/documents/why-keycloak/?utm_source=pocket_saves

[24] Keycloak Community, OpenID Verifiable for Credential Issuance, available at: https://github.com/keycloak/keycloak-community/blob/main/design/OID4VCI.md

[25] Sphereon SIOP-OID4VP, available at: https://github.com/Sphereon-Opensource/SIOP-OID4VP

[26] WooCommerce, available at: https://wordpress.org/plugins/woocommerce/

[27] Lauritz Holtmann, “Single Sign-On Security:Security Analysis of real-life OpenID Connect Implementations”, Master's thesis, 2020

[28] N. Naik and P. Jenkins, "Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect," 2017 11th International Conference on Research Challenges in Information Science (RCIS), Brighton, UK, 2017, pp. 163-174, DOI

[29] Singh, J., Patel, C., Chaudhary, N.K. (2024). Resilient Risk-Based Adaptive Authentication and Authorization (RAD-AA) Framework. In: Patel, S.J., Chaudhary, N.K., Gohil, B.N., Iyengar, S.S. (eds) Information Security, Privacy and Digital Forensics. ICISPD 2022. DOI.

[30] Jorge Navas, Marta Beltrán, Understanding and mitigating OpenID Connect threats, Computers & Security, Volume 84, 2019, Pages 1-16, ISSN 0167-4048,DOI.

[31] Fritsch, L. (2017). Privacy dark patterns in identity management. In Open Identity Summit (OID), 5-6 october 2017, Karlstad, Sweden. (pp. 93-104). Gesellschaft für Informatik

[32] Sassetti, G., Sharif, A., Sciarretta, G., Carbone, R., & Ranise, S. (2023, July). Assurance, Consent and Access Control for Privacy-Aware OIDC Deployments. In IFIP Annual Conference on Data and Applications Security and Privacy.

[33] Li, W., & Mitchell, C. J. (2020, September). User access privacy in OAuth 2.0 and OpenID connect. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 664-6732).

[34] Carsten Baum et al. “SoK: Privacy-Enhancing Technologies in Finance”, Cryptology ePrint Archive, 2023/122, DOI

[35] Scikit-fuzzy, available at: https://github.com/scikit-fuzzy/scikit-fuzzy

[36] Managing Policies in Keycloak, available at: https://www.keycloak.org/docs/24.0.1/authorization_services/#_policy_overview

[37] Policy Enforcement Point (PEP) in Keycloak, available at: https://www.keycloak.org/docs/24.0.1/authorization_services/#_enforcer_overview

[38] Python py-evm, available at: https://github.com/ethereum/py-evm

[39] ForkBomb, DIDroom, available at: https://forkbomb.solutions/solution/didroom/

[40] Keycloak extensions, available at: https://www.keycloak.org/extensions.html

[41] Plugins in Keycloak, available at: https://dev.to/yakovlev_alexey/how-to-create-a-keycloak-plugin-3acj

[42] B. Yousra, S. Yassine, M. Yassine, S. Said, T. Lo’ai and K. Salah, "A Novel Secure and Privacy-Preserving Model for OpenID Connect Based on Blockchain," in IEEE Access, vol. 11, pp. 67660-67678, 2023, DOI

[43] S. Fugkeaw, "Achieving Decentralized and Dynamic SSO-Identity Access Management System for Multi-Application Outsourced in Cloud," in IEEE Access, vol. 11, pp. 25480-25491, 2023, DOI