



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

---

## D2. DETAILED TECHNICAL SPECIFICATION OF THE SOLUTION, SOFTWARE IMPLEMENTATION WORK PLAN, DEMO SCENARIOS, THE NUMBER OF END USERS THAT WILL BE INVOLVED IN ANY PILOTS, AND PRELIMINARY BUSINESS PLAN

---

OIDC-PRINCE

---

---

Due date	10/05/2024
----------	------------

---

Submission date	17/05/2024
-----------------	------------

---

Version	1.0
---------	-----

---

Authors	Bruno Sousa (UC) Bernardo Arzileiro (UC) Tiago Galvão
---------	---

---

---

## EXECUTIVE SUMMARY

---

OIDC-PRINCE includes an architecture to enable the support of GDPR compliance proofs in the authentication and authorization processes. Such compliance, along with the requested claims are used to determine the risk associated with the shading of such information as per the profile of a service.

To evaluate the OIDC-PRINCE, a group of 8 persons has already been approached to participate and provide feedback, that will be introduced in early phases of development.

---

## TABLE OF CONTENTS

---

1	INTRODUCTION .....	8
2	USER STORIES AND USE CASE ANALYSIS (FINAL) .....	9
2.1.1	Education.....	9
2.1.2	ONLINE Selling Platform (OSP) .....	10
3	SOFTWARE DESIGN AND ANALYSIS, COMPONENT SPECIFICATION (FINAL) .....	12
4	SOFTWARE MODULES .....	14
4.1.1	Risk Module.....	14
4.1.2	Policy Module .....	15
4.1.3	EVM Client.....	17
4.1.4	Other Modules .....	18
4.2	ARCHITECTURE DIAGRAM .....	21
5	DETAILED API SPECIFICATION (PRELIMINARY) .....	23
5.1	API SPECIFICATION FOR SDK MODULES .....	23
5.2	API SPECIFICATION FOR REST SERVICES.....	23
5.2.1	RISK MODULE (REST APIS FOR THIS SERVICE) .....	23
5.2.2	EVM CLIENT (REST APIS FOR THIS SERVICE) .....	25
6	DETAILED WORK PLAN FOR IMPLEMENTATION AND DEPLOYMENT (FINAL) 27	
6.3	RISK ANALYSIS.....	31
7	BUSINESS MODEL AND EXPLOITATION PLAN (PRELIMINARY) .....	33
7.1	BUSINESS MODEL DESCRIPTION .....	33
7.2	BUSINESS VALUE FOR THE BLOCKCHAIN AND SSI DOMAIN IN GENERAL...	34
7.3	BUSINESS VALUE AND RELEVANCE FOR TRUSTCHAIN.....	34
7.4	ANY OTHER IMPACT .....	35
8	EARLY USER ENGAGEMENT PLAN .....	36
8.1	USER ENGAGEMENT ROADMAP .....	36
8.2	SAMPLE.....	36

9	CONCLUSIONS .....	38
---	-------------------	----

---

## LIST OF FIGURES

---

FIGURE 1 - POLICY ENFORCEMENT POINT IN KEYCLOAK (SOURCE [2]) .....	16
FIGURE 2 - KEYCLOAK PAGE WITH SUPPORT FOR VERIFIABLE CREDENTIALS .....	18
FIGURE 3 - OIDC-PRINCE ARCHITECTURE .....	21
FIGURE 4 - GANTT DIAGRAM .....	27
FIGURE 5 - GANTT DIAGRAM FOR T3 TASK .....	29
FIGURE 6 - GANTT DIAGRAM FOR T4 AND T5 TASKS .....	31
FIGURE 7 - STANDARD LOGIN WITH OPENID CONNECT .....	40
FIGURE 8 - LOGIN WITH OIDC-PRINCE .....	40
FIGURE 9 - STANDARD CONSENT DIALOG IN OIDC .....	41
FIGURE 10 - CONSENT DIALOG WITH OIDC-PRINCE .....	41
FIGURE 11 - CONSENT WITH OIDC-PRINCE WITH ADDITIONAL INFORMATION TO THE USER .....	42

---

## LIST OF TABLES

---

TABLE 1 - OPENID CONNECT CORE SPECIFICATION CLAIMS.....	12
TABLE 2 - OPENID CORE SPECIFICATION ADDRESS CLAIM.....	13
TABLE 3 - USERS PARTICIPATING AS VOLUNTEERS .....	36

---

## ABBREVIATIONS

---

ABAC	Attribute Based Access Control
DID	Decentralized Identifier Document
DPV	Data Privacy Vocabulary
DLT	Distributed Ledger Technology
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
RBAC	Role Based Access Control
RDF	Resource Data Format
SIOF	Self-Issued OpenID Provider
SKOS	Simple Knowledge Organization System
SSI	Self-Sovereign Identity
SSO	Single Sign On
TCP	Transmission Control Protocol

---

## 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.

The OIDC-PRINCE architecture includes the policy, risk and EVM client modules. The policy component is responsible for the enforcement of policies, as per the risk determined by the risk component. The EVM client is an auxiliary module that provides the means to allow the retrieving and storage in the blockchain.

OIDC-PRINCE in the co-creation strategy has identify **8 persons** to help in the design and evaluation of the OIDC-PRINCE solutions. The persons have different profiles in terms of IT expertise and cybersecurity. Mockups with the design of the main solutions have already been drawn to request user feedback in the early phases of development.



---

## 2 USER STORIES AND USE CASE ANALYSIS (FINAL)

---

D1 documented two types of use cases: Education and Online Selling Platform (OSP).

---

### 2.1.1 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.

---

## **2.1.2 ONLINE Selling Platform (OSP)**

---

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 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 is 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.

---

### 3 SOFTWARE DESIGN AND ANALYSIS, COMPONENT SPECIFICATION (FINAL)

---

OIDC-PRINCE leverages on OpenID Connect (OIDC) to allow Single Sign On (SSO). A relevant aspect of the OIDC-PRINCE is the claims providing details about a user's identity that can have associated privacy risks. These claims are summarized in the following tables.

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. 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 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 locale in IANA format. Example website#de to designate website in German.

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		
country	string	

---

## 4 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.

---

### 4.1.1 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

The initial validation of the fuzzy models in the risk module 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.

Risk Module developed in Python:

- With the use of Python, the Risk Module will be developed to enhance the risk assessment capabilities.
- Python provides a vast extension of libraries, which enable robust and scalable solutions that are useful for building risk models, performing simulation and for statistical analyses to assess risk exposure, such as the Python SciPy as mentioned before.
- The module will employ Fuzzy Models to evaluate the risk associated with access authorization, considering all the factors that were exposed in this topic earlier, including the service type, and sensible information (claims) that it

requires, compliance with GDPR and other interactions with the OIDC Provider.

Risk Module with API to provide risk information:

- This API will be working along with the Python implementation of the Risk Module, delivering risk information in a user-friendly manner, ensuring transparency regarding the authentication claims requested by the OIDC Provider.
- It is going to have a crucial significance for the users, by providing them with comprehensive risk details about the authentication claims that are required from them.
- The API will be able to grant the users confidence to authenticate on the services which use this provider, since they are always aware of the information that is being used by the provider.

---

#### 4.1.2 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 [1]:

- 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 1. This policy module will specify the policies for the PEP enforcement actions.

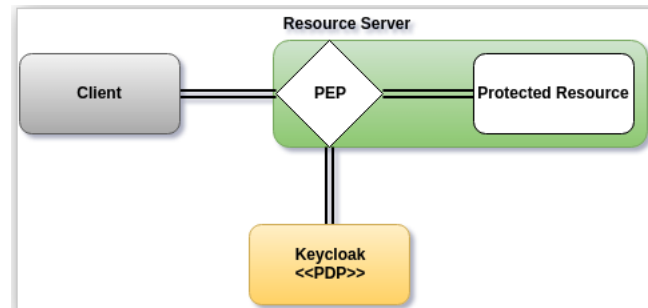


FIGURE 1 - POLICY ENFORCEMENT POINT IN KEYCLOAK (SOURCE [2])

The Policy Module will rely on JavaScript policies as they allow different modes of access control, including Attribute Based Access Control (ABAC) and Role Based Access Control (RBAC).

The Policy Module can perform the actions grant or deny depending on the Evaluation instance [3]. The example bellow, demonstrate the process on how the policies can be implemented in a RBAC mode, where the user must have the role of admin and the profile belongs to education.

```
var context = $evaluation.getContext();
var identity = context.getIdentity();
var attributes = identity.getAttributes();
var email = attributes.getValue('profile').asString(0);

if (identity.hasRole('admin') || profile.contains('education')) {
    $evaluation.grant();
}
```

LIST 1 - EXAMPLE OF CODE FOR RBAC POLICY (ADAPTED FROM [3])

This component will gather the claims information, the information stored in the EVM blockchain regarding the service, mainly GDPR proof and type of service, to request a risk analysis from the Risk module.

As per the determined risk, policies can deny or grant access to specific resources, according to the example of code mentioned in LIST 1.



---

### 4.1.3 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.

The EVM Client performs the following operations:

1. Create (C):
  - Upload Risk Data to EVM Blockchain, Compliance with GDPR and DPV.
  - Utilize the EVM client to interact with the blockchain and store the new risk entry and GDPR compliance as a transaction or smart contract.
2. Read (R):
  - Retrieve Risk Data, GDPR Compliance, and DPV: Develop features to fetch and display existing risk entries and GDPR compliance from the EVM blockchain.
  - Implement logic to query the blockchain for specific risk entries using identifiers or attributes.
  - Display the retrieved risk data within the relying party or OIDC provider interface.
3. Update (U):
  - Utilize the EVM Client to submit transactions or invoke smart contract methods to update the corresponding risk entry.
4. Delete (D):
  - Delete Risk Data from EVM Blockchain: Implement functionality to delete unwanted risk entries from the EVM blockchain.

#### 4.1.4 Other Modules

OIDC-PRINCE will leverage on the developments performed by other projects, which seek the support of SIOP [4], OIDC4VC [5] in OpenID Connect. As presented in D1, these specifications are relevant towards the support of Decentralized Identifiers (DIDs) [6]. The SIOP or Self-Issued OpenID Provider are personal OpenID Providers that issue self-signed ID Tokens, enabling portability of the identities among providers. The OIDC4VC provides an integration for Verifiable Credentials into Keycloak and it allows managing potential receivers of Verifiable Credentials as SIOP Clients. A user wallet can enable users to receive, share, and store Verifiable Credentials, manage DIDs and their related keys and view tokens.

OIDC-PRINCE, as per D1 identified the FIWARE keycloak-vc-issuer project [10] as the base project, due to its support for SIOP and OIDC4VC. As per the project owner, the SIOP support will be integrated in a future release of Keycloak. The main page of Keycloak with the support of Verifiable credentials is demonstrated in Figure 2.

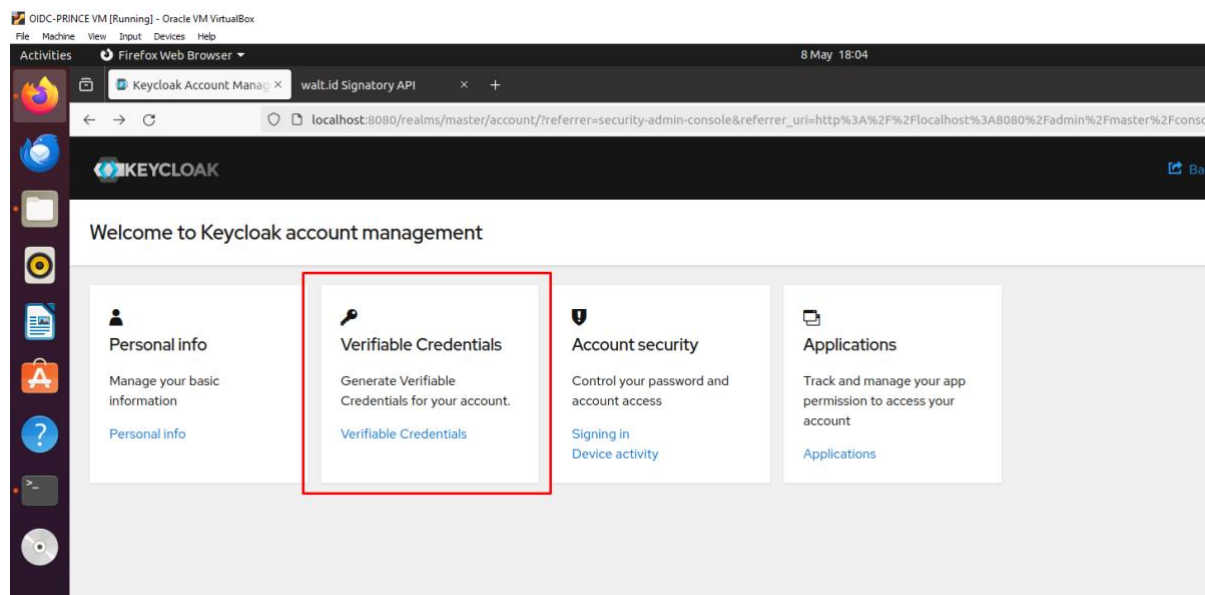


FIGURE 2 - KEYCLOAK PAGE WITH SUPPORT FOR VERIFIABLE CREDENTIALS

Adding support of Data Privacy Vocabulary (DPV) [7] and the respective GDPR [8] and risk extensions [9] in DID Documents, might require the adaptation of components dealing with DID information. An example of the DPV compliance of a service is illustrated in the following list, this information is to be stored in the EVM blockchain and to be referenced in the DIDs of the Online Shopping Service.

```

@prefix dpv: <http://www.w3.org/ns/dpv#> .
@prefix dpv-gdpr: <http://www.w3.org/ns/dpv/dpv-gdpr#> .
@prefix eu-gdpr: <http://www.w3.org/ns/dpv/eu-gdpr#> .
@prefix ex: <http://example.org/> .
@prefix dct: <http://purl.org/dc/terms/> .

# Define the online shopping service
ex:OnlineShoppingService a dpv:Service ;
    dct:title "Online Shopping Platform" ;
    dpv:hasProcessing ex:OrderProcessing, ex:MarketingProcessing ;
    eu-gdpr:GDPRLawfulness eu-gdpr:GDPRCompliant .

# Define order processing activity
ex:OrderProcessing a dpv:Processing ;
    dct:title "Order Processing" ;
    dpv:hasPurpose dpv:OrderFulfillment ;
    dpv:hasLegalBasis dpv-gdpr:Contract ;
    dpv:hasDataSubject ex:Customer ;
    dpv:usesPersonalData ex:CustomerOrderData .

# Define the data subject
ex:Customer a dpv:DataSubject ;
    dct:title "Customer" .

# Define the personal data categories for order processing
ex:CustomerOrderData a dpv:PersonalData ;
    dct:title "Customer Order Data" ;
    dpv:hasCategory dpv:IdentificationData, dpv:ContactData, dpv:FinancialData .

```

## LIST 2 - RDF EXAMPLE OF GDPR COMPLIANT FOR ONLINE SHOPPING SERVICE

The GDPR compliance information can be referenced in a DID document of the Online Shopping Service, as demonstrated in the following list, using the

alsoKnownAs and service properties.

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:oidc-prince:online-shopping-service",
  "alsoKnownAs": [ "https://oidc-prince.com", https://socialmedia.com/online-shopping-service ],
  "verificationMethod": [ {
    "id": "did:oidc-prince:online-shopping-service#keys-1",
    "type": "Ed25519VerificationKey2018",
    "controller": "did:oidc-prince:online-shopping-service",
    "publicKeyBase58": "GfH54LzH4fHJ89h4jKj54uGh5L4GhHjGfGh5JkL4Gh5J"  } ],
  "authentication": [ "did:oidc-prince:online-shopping-service#keys-1" ],
  "service": [ {
    "id": "did:oidc-prince:online-shopping-service#order-service",
    "type": "OrderService",
    "serviceEndpoint": "https://oidc-prince.com/orders",
    "eu-gdpr": "dpv:oidc-prince:online-shopping-service"
  } ]
}
```

### LIST 3 - DID EXAMPLE REFERENCING THE DPV DOCUMENT

The components used in OIDC-PRINCE like OIDC4VC, SIOP might need modifications to support adding/processing information in the DID properties of service (which allows extensions as per DID base specification [6]).

## 4.2 ARCHITECTURE DIAGRAM

The overall architecture of OIDC-PRINCE is depicted in Figure 3.

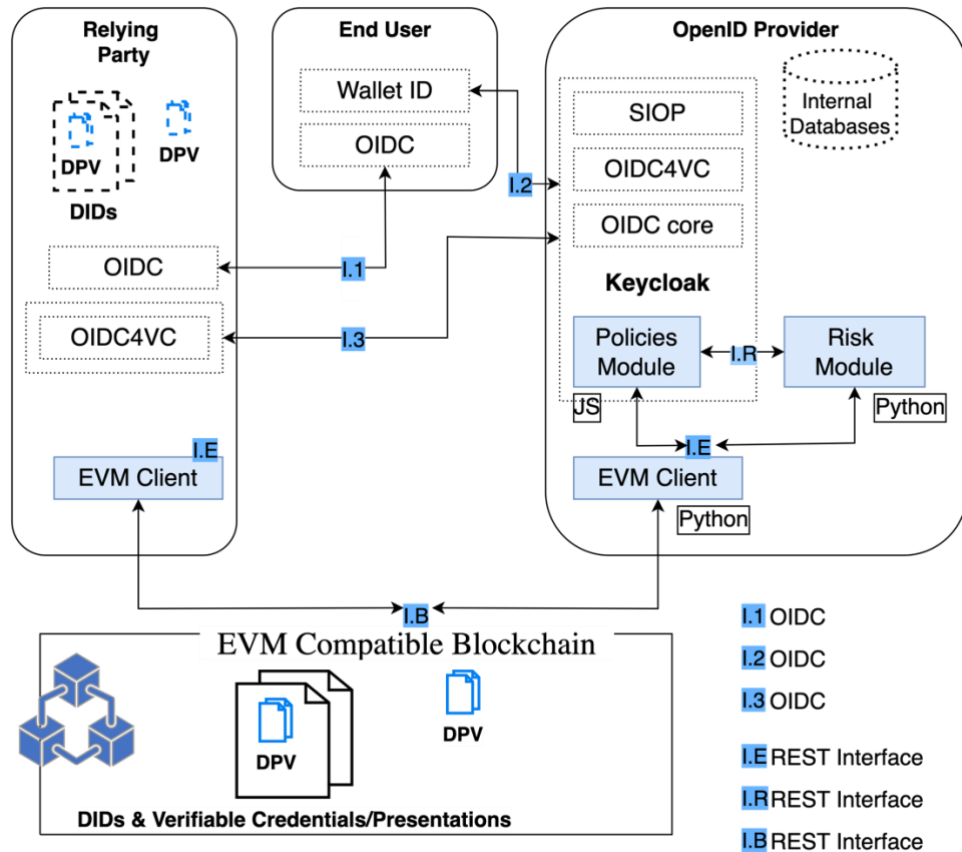


FIGURE 3 - OIDC-PRINCE ARCHITECTURE

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
- I.E – interface for other components to interact with EVM client to perform CRUD operations on the EVM blockchain.
- I.R – interface for risk management.

---

## 5 DETAILED API SPECIFICATION (PRELIMINARY)

### 5.1 API SPECIFICATION FOR SDK MODULES

---

*Describe here only the SDK modules at the API level, if applicable. If your implementation does not include SDK modules, simply write the sentence “No SDK in this implementation”, without deleting this paragraph, to preserve the structure of your document.*

**No SDK in this implementation**

---

## 5.2 API SPECIFICATION FOR REST SERVICES

---

*Describe here only the REST APIs for your services, if applicable. If your implementation does not include services, simply write the sentence “No Services in this implementation”, without deleting this paragraph, to preserve the structure of your document.*

The modules in OIDC-PRINCE that provide REST interfaces are:

- Risk module
- EVM Client

The Policies module leverages on these APIs either to provide information to the risk module to retrieve risk information and with the EVM client to retrieve information of the associated GDPR proofs.

---

### 5.2.1 RISK MODULE (REST APIS FOR THIS SERVICE)

---

The risk module is responsible to determine the risk of a specific context (required claims), GDPR compliance of the service and the profile of the service.

**Description:**

The risk module is responsible for providing risk information regarding the context, profile of service and GDPR compliance.

Endpoint: [https://<base\\_uri>/v1/risk/](https://<base_uri>/v1/risk/)

Headers:

DIDEntity: "ID value of the DID identifying the service"

The planned endpoints are documented in the following table.

HTTP method	URI	Arguments	Return value	Description
POST	/risk	(JSON) data: this argument will inform which claims is the OIDC Provider is trying to have access to.  (example of the code, it will track which claims are being accessed by the provider and puts them into a JSON object) data = { "basic_claims": { "sub": "False", "name": "True", "nick_name": "False", .... }, "address_claims": { "formatted": "False", "street_address": "True", "postal_code": "Truse", ... } }	(JSON)  (example of the response)  Response = { "risk_level": "medium", "claims_array": ["username", "phone_number", "address"] }	Returns risk level (Low, Medium or High) and will inform the user about the claims that are trying to be accessed by the provider, having in consideration the service that is user is trying to access
GET	/		(JSON) Returns 200 OK	For healthy conditions checking. For possible deployment in K8S.



---

## 5.2.2 EVM CLIENT (REST APIS FOR THIS SERVICE)

---

The EVM Client is responsible to make the interface with the EVM blockchain. This allows OIDC-PRINCE to use different type of blockchains, if required, while minimizing the required modifications for such support.

### Description:

The EVM client receives requests from other modules to perform CRUD operations regarding the DPV proofs of GDPR compliance.

Endpoint: [https://<base\\_uri>/v1/evmClient/](https://<base_uri>/v1/evmClient/)

### Headers:

DIDEntity: "value of DID identifying the service"

DIDGDPREntity<sup>1</sup>: "value of DID identifying the entity attesting the proof of GDPR"

The planned endpoints are documented in the following table.

HTTP method	URI	Arguments	Return value	Description
POST	risk	(DPV/JSON) <u>DPV document</u>  Example ex:CreateRiskEntry rdf:type dpv:DataController; dpv:hasPersonalDataHandling ex:NewRiskEntry; dpv:hasPurpose dpv:RiskManagement	(JSON) result of the operation	Create a new risk entry in the EVM blockchain
POST	dpv	(DPV/JSON)	(JSON) result of the	Create a new risk entry in

---

<sup>1</sup> This field is relevant in real use cases, where the identify attesting/auditing the GDPR compliance of an organization/service provides the level of compliance and the respective proof for such compliance.

		<u>DPV Document</u>  Example: 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. ex:ServiceA rdf:type dpv:Service ; eu-gdpr:GDPRLawfulness eu- gdpr:GDPRCompliant.	operation	the EVM
GET	dpv/		(JSON) with statistics information of DPV documents	Returns the statistics associated with the information.
GET	/risk/<id>	(DID) id: DID identifier	(JSON) DPV document (as exemplified in POST request)	Returns the resource associated to risk information
GET	/dpv/<id>	(DID) id: DID identifier	(JSON) DPV document (as exemplified in POST request)	Returns the resource associated to DPV information
GET	/		(JSON) Returns 200 OK	For healthy conditions checking. For possible deployment in K8S.

## 6 DETAILED WORK PLAN FOR IMPLEMENTATION AND DEPLOYMENT (FINAL)

The team 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 4.

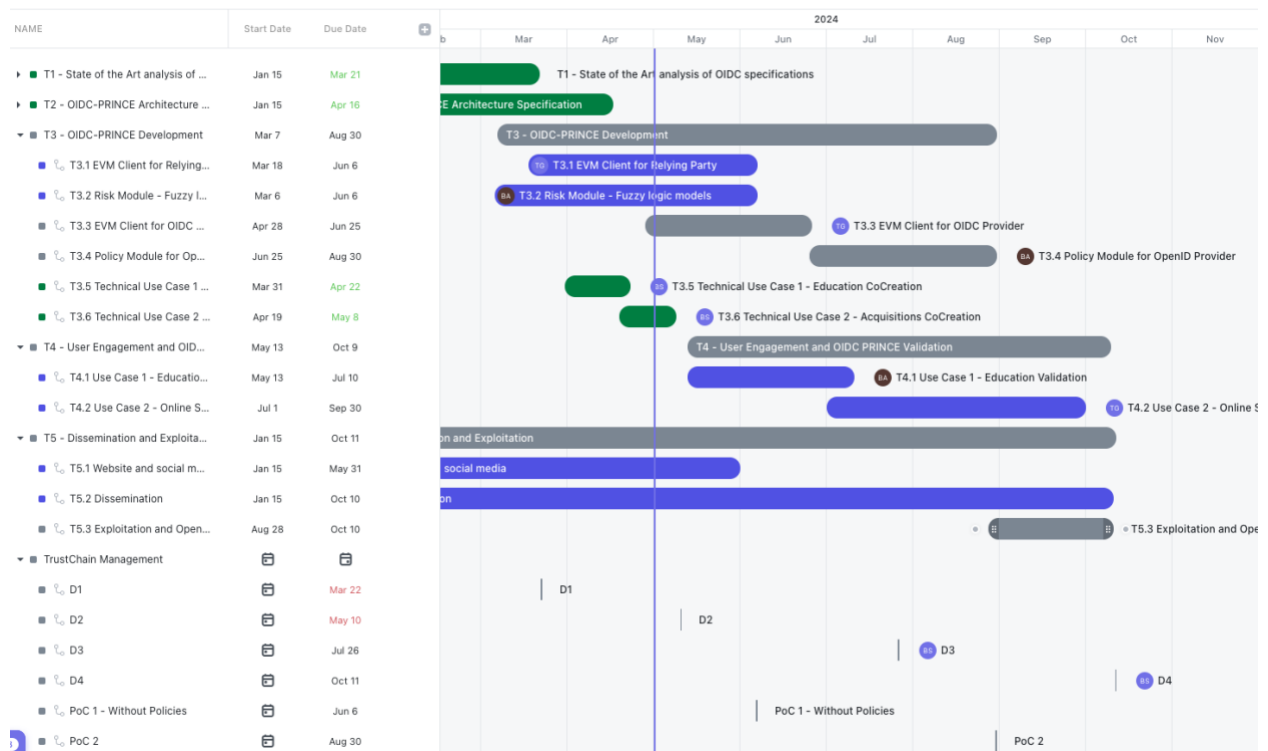


FIGURE 4 - GANTT DIAGRAM

The overall tasks of the project plan are presented in Figure 4. With the writing of this document T1 with the state-of-the-art analysis is concluded. T2 with the specification of the final architecture is also concluded. The development task T3, is partially implemented (33%).

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 June/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.

## 6.1 WORK PLAN FOR IMPLEMENTATION

The implementation is mainly performed in T3, with the following subtasks:

- 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 woocommerce 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 5 details the overall Gantt diagram for the implementation tasks.

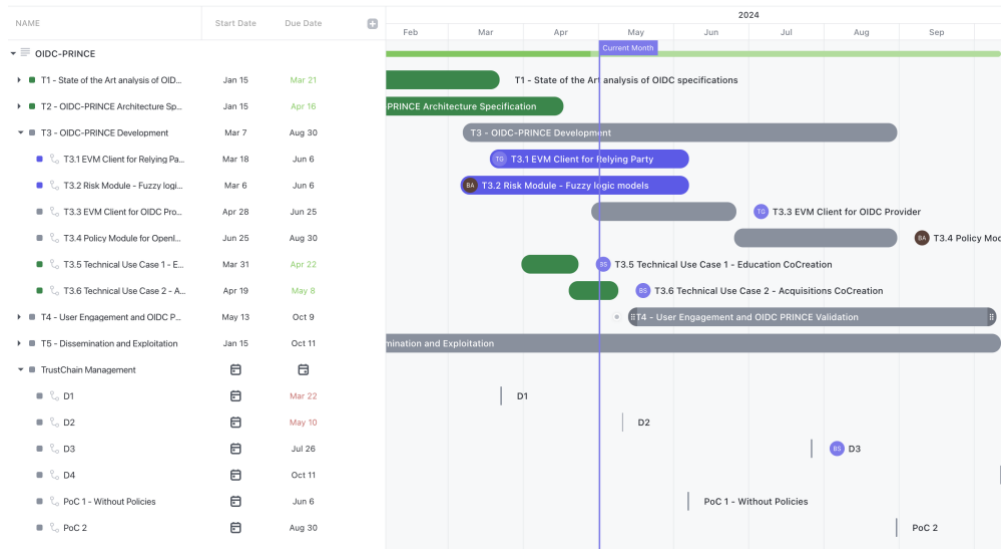


FIGURE 5 - GANTT DIAGRAM FOR T3 TASK

## 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 serves 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)
- 1st International Workshop on Fostering a Human-Centered, Trustworthy and Sustainable Internet (TRUSTCHAIN 2024)<sup>2</sup>
- 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> -- Official 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 6 shows the detailed Gantt diagram for these two tasks.

---

<sup>2</sup> A submission is being prepared at the writing of this deliverable.

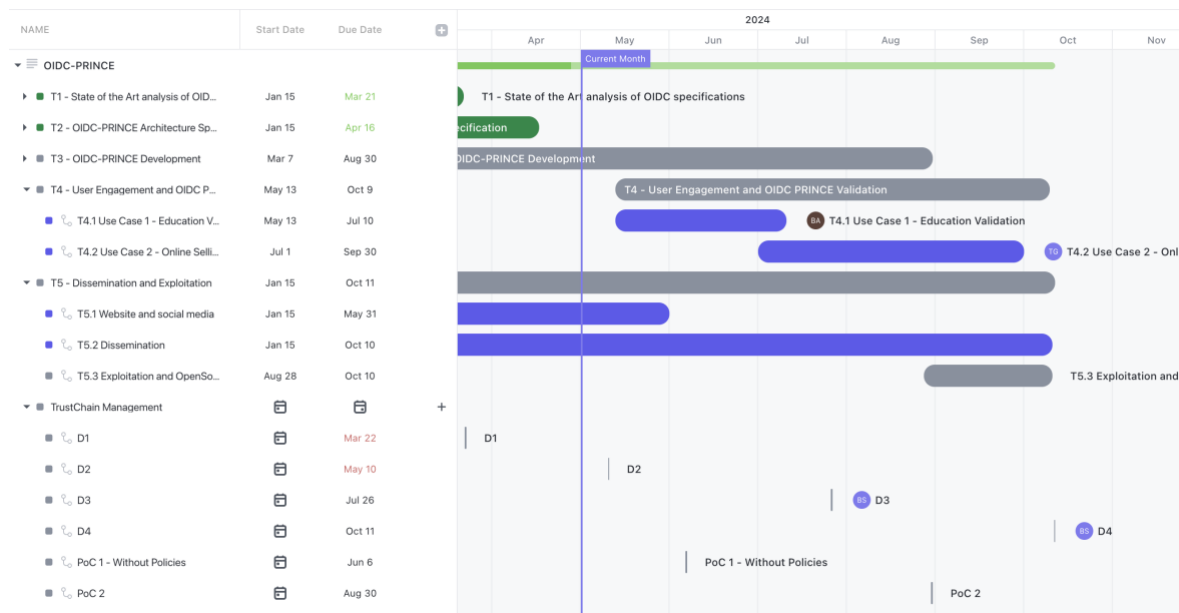


FIGURE 6 - GANTT DIAGRAM FOR T4 AND T5 TASKS

## 6.3 RISK ANALYSIS

The following risks are identified:

- **R1 – Technical issues with SIOP, OIDCVC in Keycloak**

Description: Issues in the implementation of such standards/protocols in Keycloak compromise the success of OIDC-PRINCE. DIDs will not be supported!

Mitigation: To mitigate this risk, we have already evaluated the base support project the Keycloak-vc [10] and contacted the main developer for support. The initial tests prove a working base. AS per the discussion with Stephan, the main developer the following actions/decisions are made:

- Do not update the version of Keycloak, unless it includes the supported SIOP and OIDC4VC functionalities, as future releases will integrate the functionalities of SIOP.
- Do not use other type of wallet for DIDs, the one that is used is the walt-id [11].

- **R2 – Technical issues with the integration of DPVs in DIDs**

Description: There is the need of a connection between DPVs and DIDs. DIDs identify the identities (users, services), while DPVs provide the GDPR compliance proof of a service/organization.

Mitigation: In this regard, the current plan focusses on two possible approaches:

- a) using DID extensions in the service property to convey information of the DPV proofs.
- b) Embed the DPV in DIDs

Both approaches are being considered to mitigate possible issues in the integration of additional information on DIDs in a standard fashion

- **R3 – Delays due to holiday season**

Description: The project duration goes through the summer holiday season, where most of the members are in vacations.

Mitigation: To not further delay the implementation of the project, the periods of holidays from project members will be collected to identify the periods where less work will occur on the project. Additionally, tasks demanding more work will be anticipated.



---

## **7 BUSINESS MODEL AND EXPLOITATION PLAN (PRELIMINARY)**

---

---

### **7.1 BUSINESS MODEL DESCRIPTION**

---

The business model associated with this proposal consists in the “freemium model”, where the tools are released as open source, with support by email. The achieved outputs are expected, in a first plane to enhance the knowledge at CISUC, and thus being used in the master courses (MSI) and PhD program, due to their relevance in terms of GDPR-policy compliance and federated authentication and authorization solutions. On a second plane, the outputs of the project will be employed in the collaboration activities that the CISUC has with entities like SMEs, public organizations and others. These activities can be designed in the context of specific project proposals in Horizon Europe calls, or at national level in Portugal. Additionally, consultation activities will also include the outputs of the project namely to assist SMEs in the GDPR compliance, as well as making more robust their solutions in terms of identity management and support for federated authentication and authorization processes.

Additionally, the CISUC team will seek to further validate the results in high scale projects, pursuing financed calls at European level or other programs. In particular, the connection with ENISA towards the adoption of the proposed solution to further promote the adoption of digital identity standards by entities from different economic areas. The environmental sustainability associated with the project might be related with the use of DLT technologies to store the certified GDPR-policy compliance information. While this is planned in the project to enhance transparency and trustworthiness between different players of the OpenID ecosystem, a technical solution might not strictly require the employment of DLT. Assuming trust relations between OpenID providers and certification authorities regarding GDPR-policy compliance, other mechanisms can be used to convey the proofs of compliance with different types of technologies which integrated seamlessly with the current protocols of OpenID connect (e.g., HTTPS). Additionally, the enhancements designed in the project will be performed in a fashion to facilitate processing and for data minimization (e.g., avoiding the exchange of information not required).

---

## 7.2 BUSINESS VALUE FOR THE BLOCKCHAIN AND SSI DOMAIN IN GENERAL

---

The following values are provided to the Blockchain and SSI domain in general:

1. Consolidate federated authentication and authorization approaches based on standards like OpenID Connect that can be employed by SMEs, and industry partners with which CISUC has collaboration and research activities.
2. Accelerate the compliance with GDPR by SMEs, public institutions, service providers and increase the level of trustworthiness between services and OpenID providers by providing means to exchange certified proofs regarding GDPR compliance for sensitive operations like authentication and authorization.
3. Impact on how users of different services can perceive the risks of consenting the access to their personal data through informed consent mechanisms. Placing users as part of the solution for trustworthy and privacy-compliant data processing impacts the relations between users and services, and between users and providers for federated authentication solutions like OpenID Connect providers (e.g., Google, Facebook).

OIDC-PRINCE has impact in the domain of consent management systems, and ROPAs with verification and certification for GDPR-policy compliance. The certified GDPR-policy compliance is employed as input to accept the registration of services to access private user data. The consent management, as part of the federated authentication and authorization process of OpenID is enhanced with the privacy risk associated with the access granting to specific fields of user private data. The proposed approach, to enhance the consent process in OpenID has also the potential to be employed in others use cases that greatly benefit with the information of GDPR-policy compliance, as well as privacy risks information.

---

## 7.3 BUSINESS VALUE AND RELEVANCE FOR TRUSTCHAIN

---

The OIDC PRINCE contributes to the challenges targeted in the TRUSTCHAIN project, by enabling consent profiles, by enabling new privacy preserving data flows in the OIDC authentication and authorization processes, and by promoting the compliance with privacy regulation standards on services.

OIDC PRINCE benefits the TRUSTCHAIN project, by enhancing key protocols like OpenID Connect, that are used for authenticating. In addition, the proposed solution can also be integrated with the DLT provided in TRUSTCHAIN to hold the verifiable proof of GDPR-policy compliance.

OIDC-PRINCE has the following potential impact in TRUSTCHAIN:

1. Impact on OpenID specifications, by includes the claims validated in the project and that allow the enforcement of policies that respect more the privacy of users, by not allowing the connection of services that do not comply with privacy related standards. The reputation of CISUC can also be enhanced with the collaboration in standards related to authentication, allowing CISUC to continue as an Excellent research centre.

---

## 7.4 ANY OTHER IMPACT

---

The CISUC is a top research centre in Portugal and the most important research centre in ICT in the central region of the country, covering various topics in the fields of Computer Sciences and Informatics Engineering. Since 2019, it has been graded as Excellent, by the Foundation for Science and Technology under the R&D Units Evaluation process. CISUC contributes to the development of technologies and collaborates actively with end-users, SMEs, industry for technology and knowledge transfer, having an active role in the innovation and competitiveness of the industry.

The results of the OIDC PRINCE will create the following impact:

1. Consolidate the know-how on federated authentication and authorization solutions.
2. Enable the consolidation and validation of solutions that can increase data privacy compliance, leveraging previous solutions, and adapting them to the specificities of authentication and authorization processes.
3. Establish a baseline for CISUC to promote research and innovation project proposals in national or European funding programs.
4. Enable validation of privacy and security mechanisms in course units of a master course.
5. Enable the validation and design of advanced security mechanisms in the doctoral program.

---

## 8 EARLY USER ENGAGEMENT PLAN

### 8.1 USER ENGAGEMENT ROADMAP

---

The **8 persons** have already been approached, in informal ways (no email invitation and no detailed information has been provided). As per the planned activities in tasks T4.1 and T4.2 users will be approached during the month of May to provide initial feedback regarding how the risk information can be presented more objectively.

Additionally, users will also be engaged in the use cases. The Education use case will be the first to use the OIDC-PRINCE mechanisms to allow the validation of the risk information in platforms like Moodle.

At the end of June users will be engaged in the online selling platform to provide feedback regarding the risks associated with such type of platforms.

The user engagement has been considered in the planning of the project, as detailed in Section 0.

---

### 8.2 SAMPLE

---

The use co-creation will rely on a total of **8 persons**, as summarized in Table 3. The main concerns include persons with different IT skills and knowledge regarding cybersecurity, we also seek a balanced gender in the volunteers.

TABLE 3 - USERS PARTICIPATING AS VOLUNTEERS

Age Range	Gender	IT Skills	Academic/ Formation	N° of candidates
[18 - 25]	Male	High	Bachelors in informatics	4
[18 - 25]	Female	High	Bachelors in informatics	2
[15 - 18]	Female	Medium	Secondary School	1
> 50	Female	Low	Professional course	1

These users will be involved in the user Co-Creation that has been delineated for the two use cases:

- **Use case A – Education**

In this use case users will be asked to Register in Moodle to have access to the contents of a Massive Online Course. During the registration and authentication processes the users will be asked to provide feedback regarding the information of risks and the perceived security in terms of having information regarding the authentication process with GDPR compliance information of the Moodle service.

- **Use case B – Online Selling Platform**

In this use case users will be asked to use an online selling platform, for this, they need to register and authenticate in the platform. The platform will be configured with some goods that can be placed in a basket to be acquired. Users will be asked to provide feedback regarding the information of risks and the perceived security in terms of having information regarding the authentication process with GDPR compliance information of the Online Selling Platform.

In both use case the user feedback will be collected through specific forms to allow an analysis of the results. In some cases, the project members might help, or provide additional information to users.

As part of the co-creation process, Mockups have already been created, to gather inputs from users from the very beginning of the development activities. The Mockups are documented in Annex A.

---

## 9 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 architecture of OIDC PRINCE towards its major goal and details the final plan for the deployment and implementation of functionalities. The architecture of OIDC-PRINCE includes modules like the Risk module, the Policy Module and the EVM Client.

Details regarding the co-creation process are also documented. OIDC PRINCE team has a multidisciplinary team, with different expertise areas including privacy, risk management and authentication.

---

## REFERENCES

---

- [1] Managing Policies in Keycloak, available at: [https://www.keycloak.org/docs/24.0.1/authorization\\_services/#\\_policy\\_overview](https://www.keycloak.org/docs/24.0.1/authorization_services/#_policy_overview)
- [2] Policy Enforcement Point (PEP) in Keycloak, available at: [https://www.keycloak.org/docs/24.0.1/authorization\\_services/#\\_enforcer\\_overview](https://www.keycloak.org/docs/24.0.1/authorization_services/#_enforcer_overview)
- [3] Keycloak Evaluation API, available at: [https://wjl465150.gitbooks.io/keycloak-documentation/content/authorization\\_services/topics/policy/evaluation-api.html#\\_policy\\_evaluation\\_api](https://wjl465150.gitbooks.io/keycloak-documentation/content/authorization_services/topics/policy/evaluation-api.html#_policy_evaluation_api)
- [4] Self-Issued OpenID Provider, available at: [https://openid.net/specs/openid-connect-self-issued-v2-1\\_0.html](https://openid.net/specs/openid-connect-self-issued-v2-1_0.html)
- [5] OpenID for Verifiable Presentations, available at: [https://openid.net/specs/openid-4-verifiable-presentations-1\\_0.html](https://openid.net/specs/openid-4-verifiable-presentations-1_0.html)
- [6] W3C, "Decentralized Identifiers (DIDs)", 2022, <https://www.w3.org/TR/did-core/>
- [7] W3C, "Technology Concepts for DPV", <https://w3c.github.io/dpv/tech/>
- [8] W3C, "EU-GDPR Extension Data Privacy Vocabulary", 2023, <https://w3c.github.io/dpv/legal/eu/gdpr/>
- [9] W3C, Risk Extension for DPV, <https://w3c.github.io/dpv/risk/>
- [10] FIWARE Keycloak-vc-issuer project, available at: <https://github.com/FIWARE/keycloak-vc-issuer>
- [11] Identity by walt.id, available at: <https://github.com/walt-id/waltid-identity>

---

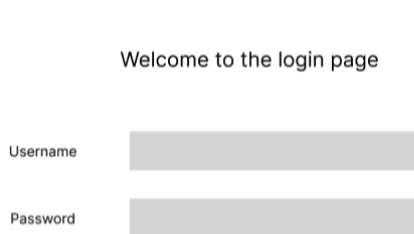
## APPENDIX A – USE CASE CO-CREATION STRATEGY

---

Initial Mockups have been drawn to accomplish the goals of the project, namely:

- Evaluate the solutions developed by OIDC-PRINCE
- Use OpenID Connect as the base line for comparison

In this regard the following Mockups will be presented to the user, to gather feedback regarding how the risk information should be present. These Mockups have been developed in Figma and are available in the following [link](#).

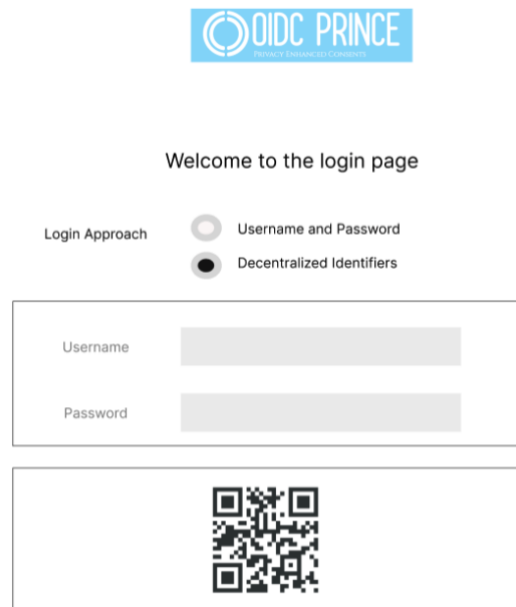


Welcome to the login page

Username

Password

FIGURE 7 - STANDARD LOGIN WITH OPENID CONNECT



Welcome to the login page

OIDC PRINCE

Login Approach

☒ Username and Password

☐ Decentralized Identifiers

Username

Password




FIGURE 8 - LOGIN WITH OIDC-PRINCE

Regarding the consent operation, as required in the Authorization flow of OAuth2/OpenID Connect, the following screens have been prepared.




The service A wants to access to the following information:

☒ Your **email address** user@domain.xpto  
☒ Your **first and last name**  
☒ Your **address**  
☒ Your **mobile phone**

Grant Access


Deny Access

FIGURE 9 - STANDARD CONSENT DIALOG IN OIDC



Consent to **Service A**

**Risk Level: 4 - HIGH** ⓘ



**Service A** is % compliant with GDPR  
(further [details](#))

Service A wants to access:

☒ Your **email address** user@domain.xpto ▲ ⓘ  
☒ Your **first and last name** ▲ ⓘ  
☒ Your **address** ▲ ⓘ  
☒ Your **mobile phone** ▲ ⓘ

Grant Access

Deny Access

FIGURE 10 - CONSENT DIALOG WITH OIDC-PRINCE

As per Figure 10 one can notice that the additional information items, namely regarding risk. Details of such risk will be provided to the user, as illustrated in the figure below.

