Heliyon 10 (2024) e28560

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

A federated authentication schema among multiple identity providers

João Rafael Almeida [a,b,*], André Zúquete [a], Alejandro Pazos [b], José Luís Oliveira [a]

[a] DETI/IEETA, LASI, University of Aveiro, Aveiro, Portugal
[b] Department of Computation, University of A Coruña, A Coruña, Spain

ARTICLE INFO

Keywords:
Federated authentication
SSO
IdP
OAuth 2.0
ELIXIR AAI

ABSTRACT

Single Sign-On (SSO) methods are the primary solution to authenticate users across multiple web systems. These mechanisms streamline the authentication procedure by avoiding duplicate developments of authentication modules for each application. Besides, these mechanisms also provide convenience to the end-user by keeping the user authenticated when switching between different contexts. To ensure this cross-application authentication, SSO relies on an Identity Provider (IdP), which is commonly set up and managed by each institution that needs to enforce SSO internally. However, the solution is not so straightforward when several institutions need to cooperate in a unique ecosystem. This could be tackled by centralizing the authentication mechanisms in one of the involved entities, a solution raising responsibilities that may be difficult for peers to accept. Moreover, this solution is not appropriate for dynamic groups, where peers may join or leave frequently.

In this paper, we propose an architecture that uses a trusted third-party service to authenticate multiple entities, ensuring the isolation of the user's attributes between this service and the institutional SSO systems. This architecture was validated in the EHDEN Portal, which includes web tools and services of this European health project, to establish a Federated Authentication schema.

1. Introduction

Online platforms and services that are accessible through users' credentials require a technical solution for the management of these credentials. Independently of the mechanisms and type of credentials adopted, each application or service needs to handle this procedure, often storing some user attributes to verify credential authenticity. However, this approach requires that users create separate accounts for each service, leading to an unmanageable set of credentials to handle. A possible solution proposed to address this issue was the creation of a unique credential system that authenticates users in multiple services, known as Single Sign-On (SSO). This strategy gained great adoption in different scenarios, including corporate environments [1], universities [2], online banking [3], and more.

SSO is an authentication strategy that allows an authorized user to log in once and grant access to multiple applications without repeating logins for each application during a single session [4]. This mechanism centralizes user accounts and facilitates the

* Corresponding author.
E-mail address: joao.rafael.almeida@ua.pt (J.R. Almeida).

https://doi.org/10.1016/j.heliyon.2024.e28560
Received 22 September 2023; Received in revised form 8 March 2024; Accepted 20 March 2024

Available online 26 March 2024

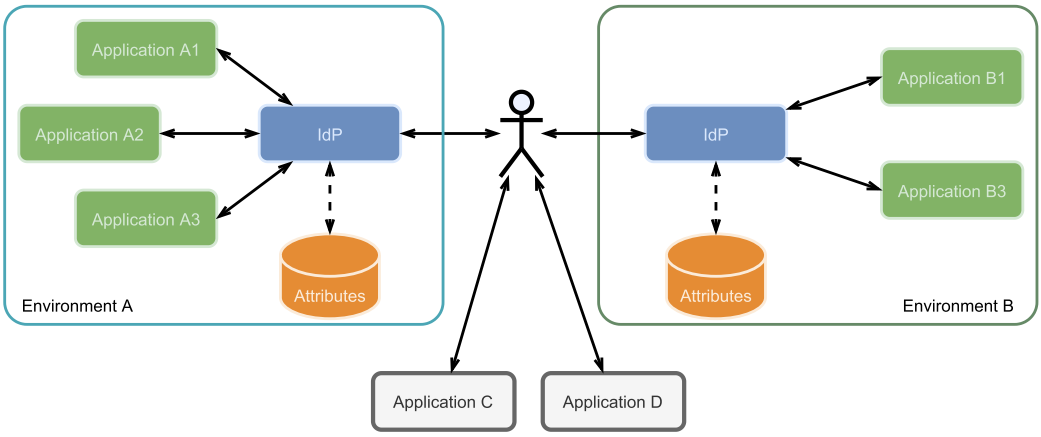

Fig. 1. Overview of the current strategy used for authenticating a user in the systems. Each environment has an individual IdP, and other applications, outside these environments, have their independent login modules.

management of user profiles [4]. It addresses the problem of handling multiple credentials in different systems within the same institutions by establishing a federated environment. Clients sign in once to the environment and gain access to the services [5].

Depending on the scenario, the implementation of SSO can bring different benefits. For instance, in a consumer-facing environment, users might enjoy SSO across multiple applications that allow them to log in via a cloud-based authentication. When considering platforms that may not support this kind of authentication mechanism, the integration of SSO is challenging [6]. The problem can be simplified by enabling the use of different protocols for authentication. However, this still requires some effort to ensure the integration of multiple tools. Another issue, when considering complex scenarios is the different levels of privileges for each application, which may lead to an unmanageable matrix of Rule-Based Access Control (RBAC) policies [7].

In an enterprise environment, an employee might take advantage of using SSO across internal and cloud applications, leveraging the company Identity Provider (IdP) for authentication. Similar situations can arise in universities, where students, lecturers, and administrators might use SSO across university applications using the university identity provider thereafter [1]. An IdP is a component in a federated identity architecture responsible for establishing, maintaining and securing the digital identity of subjects [8]. Identity is composed of attributes that characterize these subjects, and there is at least one that unequivocally identifies each [9]. On the other hand, a federated identity consists of an agreement between entities about the definition and use of those attributes [10]. In a federated identity, the user's identity is linked across multiple separate identity management systems. This allows users to move quickly between systems while maintaining security [11].

1.1. Motivation

While SSO mechanisms can simplify the authentication procedures by unifying credentials, their efficacy requires an IdP to consolidate all user attributes required across the different services. However, these mechanisms fail in scenarios that involve federated identity across diverse platforms, specifically in collaborative environments. In these scenarios, each institution operates its own SSO system paired with an IdP. This situation is frequently observed in research projects where applications are developed to meet specific objectives, without considering such details. The complexity increases if it is necessary that these applications need to be interoperable. In this case, a different approach to managing the users' identity among solutions is required that transcends the limitations of traditional SSO approaches.

A possible strategy to handle the limitations of current SSO systems in multi-institutional environments is based on using a centralized IdP. It would be responsible for managing user credentials across all applications. However, this solution presents several challenges. One of these is related to sensitive user attributes. Users might trust one specific institution with their sensitive information, but extending this trust to all institutions in the network may not be possible. Another challenge is the management of roles using a centralized IdP. This introduces the need for a dual-layered system of roles and permissions: i) one at the central IdP level; and ii) another at the individual application level. The first could implement role-based access control policies for each application to mitigate this. Under this system, a designated entity could oversee role assignments for a group of applications. However, this introduces some complexity in the initial implementation of the system and ongoing management.

Similar to the previous issues would be the process of approving new users. Depending on the project's magnitude, this process requires information about the user, the application for which access is required, and what role this user would have. Managing these attributes at the application level, or the institutional SSO level would be simpler. Additionally, the use of an already established IdP may increase the trust in that account. For instance, the one already used by a university. In these scenarios, the registration process requires more details and documents about the person that is being registered.

Therefore, the current approach to this problem is to have repeated credentials. Fig. 1 illustrates a generic example in which the user would require 4 credentials to access all the services in this ecosystem. However, applications A1, A2 and A3 would only require

one credential, since these are under the same SSO implementation, where there is a local IdP that stores the user attributes for that subsystem.

1.2. Contribution

In this work, we proposed an architecture for federated authentication across multiple SSO systems applied to healthcare projects. We aim to facilitate the integration of the existing applications without extensive modifications. Although this integration may be simple in specific domains, when considering the present scenario (that includes health data and a diversity of open-source and commercial solutions), some modifications may not be possible to implement. Therefore, our proposal is based on well-established protocols, reducing the impact of adapting software to a new solution. This approach centers on devising a strategy where a Trusted Third Party (TTP), mutually agreed upon by all participating entities, handles user accounts. This TTP stores a basic set of user attributes, while more sensitive data remains within the local infrastructure.

To demonstrate the feasibility of our solution, we integrated the ELIXIR AAI system, now transitioned to Life Science Login, as our authentication and authorization infrastructure. Provided by the Elixir organization, this framework leverages the existing institutional identities of service providers. We applied our strategy to the EHDEN Portal, which is the central hub for the activities of EHDEN project. EHDEN is a European health initiative to create a trusted research ecosystem for observational health data. The portal aims to facilitate access to a network of standardized health data sources, tools, and training materials.

2. Related work

Existing authentication protocols and SSO mechanisms are well described in the literature and applied in real contexts. Since we aim to implement a Federated Identity Management (FIdM) solution for aggregating multiple SSOs and stand-alone applications, we evaluated standards that are currently used for this task. Additionally, we evaluated authentication and authorization infrastructures as the TTP element in the proposed architecture.

2.1. Federated identity management standards

The concept of FIdM is predominantly defined in the following standards: Security Assertion Markup Language (SAML) [12], Open Authentication (OAuth) 2.0 [13] and OpenID Connect (OIDC) [14]. These standards share similar features, using security tokens in their services. The security tokens, also known as Identity Tokens, Authentication Tokens and Authorization Tokens, are the key concept in a FIdM implementation because they are responsible for authenticating and authorizing users [15].

2.1.1. Security assertion markup language (SAML)

SAML is a framework based on XML format that is used for transmitting user authentication and attribute information. This framework is composed of three entities, namely the Identity Provider (IdP), Service Provider (SP) and client (which is usually the browser) [16,12].

The IdP is the entity responsible for authenticating and authorizing clients, and issuing assertion tokens for services. The SP is the entity that relies on an IdP for processing the authentication and authorization of these services. The client is the application that starts the protocol for consuming the services provided by the SP [16,12].

Although this protocol is frequently used to implement SSO, it is not a lightweight standard. XML is a verbose representation of the messages in the protocol, and the implementation of this may require some effort. One issue is scalability, which may require the implementation of complex broker services to support multiple SP and IdP [16]. Additionally, there is a lack of open-source libraries aiming to simplify the interaction of the three entities and to create the protocol messages.

2.1.2. Open authentication (OAuth) 2.0

OAuth was developed for a different purpose from SAML. This protocol aims to enable a client application to obtain limited access to an HTTP service, or resource, on behalf of the owner of that resource. The protocol describes the flow for approving interactions between the resource owner and the HTTP service, by allowing the third-party application to obtain access on its behalf [13,17]. In this protocol, there are four entities: the resource owner; the application, defined as the client; the authorization server; and the resource server or HTTP service.

The resource owner is the user who possesses the access rights to a resource. The user is the entity capable of granting access to their protected resources. The resource server hosts the protected resources and can respond to requests for these resources using a valid access token. The authorization server is the entity that issues the access token. Finally, the client is the application that wants to access the protected resources, usually on behalf of the resources' owner.

Although this protocol was developed aiming to delegate permission to others to access protected resources, this can be used for an SSO implementation. This protocol is the most commonly used standard for delegating authentication in applications and services on the Internet. For instance, well-known identity providers supporting this standard are Facebook, Twitter or Google [18].

Compared to SAML 2.0, OAuth is lighter, more scalable, and can be more easily integrated into multiple online services and platforms. From an architectural design and security perspective, OAuth suits better with the most relevant FIdM approaches [18,15].

Table 1
Overview of the most common Federated Identity Management Standards and Trusted Third Party Authenticators.

	Technology	Description
FIdM Standards	SAML	XML-based standard for exchanging authentication and authorization data.
	OAuth 2.0	Authorization framework for third-party access to user accounts.
	OIDC	Simple identity layer on top of OAuth 2.0 protocol. Common in consumer-focused services like social media logins.
TTP	ELIXIR AAI	Framework for federated authentication and authorization in life sciences. Used in life science research for accessing services.

2.1.3. OpenID connect (OIDC)

The OIDC is an extension of the OAuth 2.0 protocol, more precisely an identity layer on the top of this protocol [18,14]. This framework contains a group of specifications for transmitting users' identity using RESTful services [14] and facilitates the process of clients confirming the users' identity depending on a chosen OAuthe 2.0 Authorization Server.

This protocol involves three parties, namely the IdP, the Relying Parties (RP) and the users. The IdP manages users' accounts and authenticates them. An authenticated user can request an access token in the IdP to use it to log in to the RP [14]. Even though OIDC has more features than OAuth 2.0, some older systems only support the latter in their authentication components.

2.2. Trusted third party authenticators

SSO uses a common authentication and authorization infrastructure that was represented by the IdP in the previously described protocols. However, there are public infrastructures to acquire this role, namely Google, Facebook and Microsoft, among others [19].

In the context of health research projects, it is not possible to rely upon these public identity providers for several reasons. One is the lack of user verification, *i.e.*, anyone can create a fake account in one of these applications in a few minutes. Therefore, in projects where there is sensitive information and the consortium is restricted to members of specific organizations, these public infrastructures fail.

In Europe, ELIXIR AAI was developed to implement SSO in services that have been identified as a key enabler for European bioinformatics [20]. ELIXIR aims to ensure interoperability between the bioinformatics tools, data resources and cloud services existing in Europe to facilitate scientific discoveries. This is only possible if these components follow the FAIR principle by being findable, accessible, interoperable and reusable [21].

ELIXIR is currently connecting national bioinformatics networks, known within ELIXIR as Nodes.[1] The Nodes affect the direction of ELIXIR based on the national priorities of each one, as has been described by ELIXIR Netherlands [22], ELIXIR Norway [23] and ELIXIR Switzerland [24]. The goal of this infrastructure is to expand the resources in the ecosystem to all entities involved. This has resulted in partnerships between industry and academia, which have had a positive impact on scientific research [25]. Industrial users range from small and medium-sized enterprises (SMEs) to large multinationals, covering the pharmaceutical, healthcare, food, agriculture and blue biotech sectors. [25].

The ELIXIR authentication and authorization services (ELIXIR AAI) allow the use of users' institutional credentials to sign in. For instance, a researcher can use the university credentials stored in the institutional IdP to log in to this infrastructure. This increases users' authenticity since researchers' identities are usually verified by the organizational services with government documents or face-to-face checking. Although this is not invulnerable, these mechanisms create a new layer of security to avoid fake accounts.

2.3. Summary

In this section, we summarize the protocols and technologies previously presented. Table 1 provides a more comprehensive overview of related works conducted on federated identity management.

3. Methods

The proposed architecture was designed to create a federated identity management in health projects. This incorporates some of the previously described protocols and ELIXIR AAI. In this section, we present this architecture and the registration and login flow in this environment.

3.1. Proposed architecture

The goal of creating a federated identity over multiple platforms can be accomplished by implementing an SSO mechanism split into layers. Fundamentally, the idea is to have a centralized infrastructure responsible for reusing existing institutional identities and provide access tokens to allow users to be authenticated in the platforms and services used in the project. Users' more sensitive

[1] https://elixir-europe.org/about-us/who-we-are/nodes.

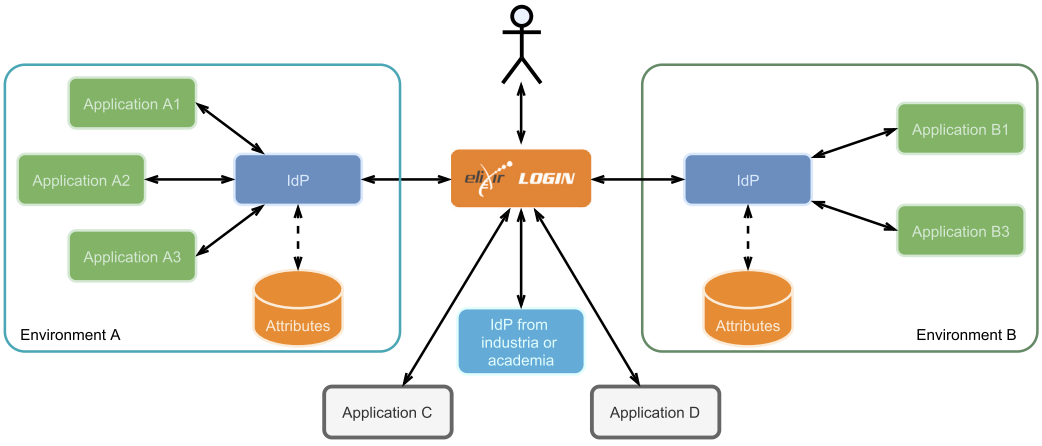

Fig. 2. Overview of the proposed architecture using a trusted third party system (ELIXIR AAI) as an account manager and keeping all IdP and the more confidential attributes inside each environment.

attributes or those specific to a service are kept in that service. For instance, a platform that provides question/answering services, like a forum, does not require the same attributes as administrative services do. Therefore, these attributes should be kept locally.

The architecture is composed of four distinct entities, each playing a crucial role in the system's functionality:

1. Users: These are individuals who require access to the services of the project. These can be project stakeholders, namely researchers and administrative personnel (each with different levels of access and privileges).
2. Institutional services: These services are the applications that users need to access, namely a web portal containing project information and remote services protected by credential-based security. These institutional services represent the end targets for user authentication.
3. Centralized authentication and authorization infrastructure: This infrastructure is the key component of the architecture. It aims to centralize and manage user accounts and roles. It serves as an intermediary, interacting with the authentication components of each institutional service.
4. Industrial or Academic IdP Services: Aligned with ELIXIR AAI standards, these services aim to store the users' credentials at each institution.

In this architecture, users predominantly rely on ELIXIR login and their institutional IdP for accessing all project-related services. The overall process between these components and their contribution to streamlining the access to each service is illustrated in Fig. 2. In the end, credentials are still kept in the institutional IdP, but a centralized service makes the bridge between them and the services that require authentication.

3.2. Protocols

In the integration of ELIXIR with applications using OIDC, we need to define four specific scopes. Each scope represents a distinct category of user information. These are the following:

- "voperson_external_affiliation": This scope contains to the users' affiliations. It enables the system to recognize the users' external professional or academic connections. For instance, collaborations with other researchers.
- "openid": It is used to initiate the OpenID authentication process, namely the user's consent to authenticate using this protocol. This scope is critical for the basic operation of the OIDC protocol within the system.
- "email": It grants the application access to the user's email address. It is used in the applications as the user identity. Some of them may require this field for communication and notifications.
- "profile": It includes basic profile details like the user's name, profile picture, and other personal information that can be used for identification and personalization purposes within each application. Users can decide which attributes will be shared during the registration step.

These scopes enable the institutional IdPs to provide user attributes aligned with each scope. This structure ensures that each user's access rights and experiences are appropriately configured according to their specific roles, affiliations, and identity information.

For applications not supporting OIDC or OAuth 2.0, an alternative pathway involves using SAML. However, this alternative was not adopted in our implementation. Services incompatible with any of these protocols (OIDC, OAuth 2.0, or SAML) would require updates in their authentication mechanisms.

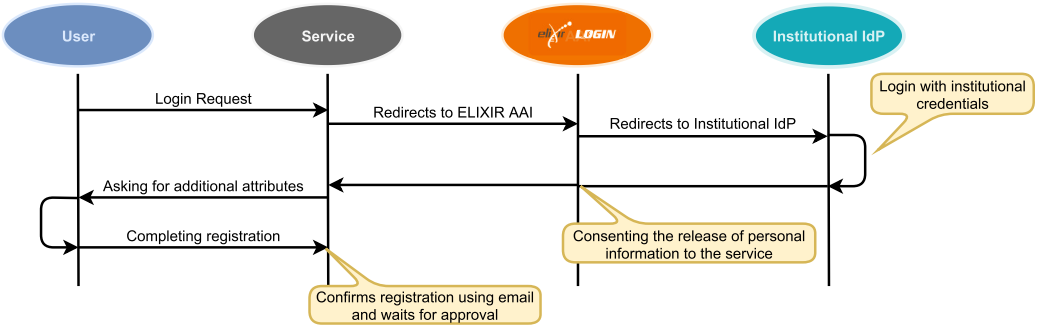

Fig. 3. Overview of the registration flow between the four entities to access a service. Message details were omitted.

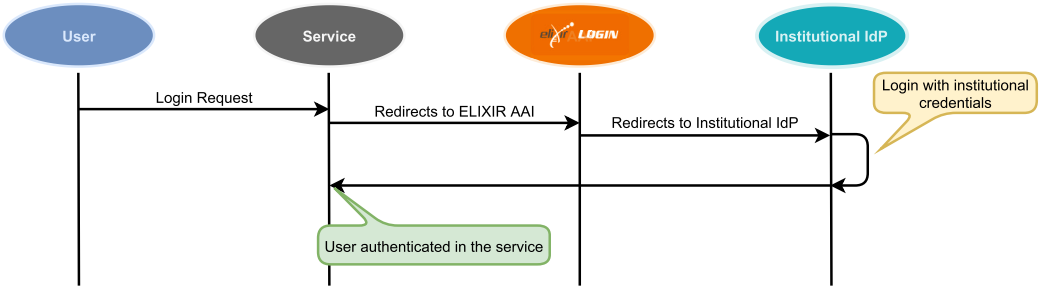

Fig. 4. Overview of the authentication flow between the four entities to access a service. Message details were omitted.

3.3. Tokens

In the OIDC implementations, the “Authorization Request”parameter encapsulates OIDC requests. Therefore, requests are conveyed in a single, self-contained JSON Web Token (JWT). In this scenario, referred to as a “Request Object”. This object can be optionally signed and/or encrypted to enhance security.

The “Request Object”to be compliant with OAuth 2.0 Authorization Request norms, it must include the “response_type”and “client_id”parameters. Additionally, if the “Request Object”contains a scope parameter, it must be passed using the same syntax, including the “openid”scope.

The “Request Object”may be signed, unsigned, or encrypted. If signed, the JWT should contain “iss”(issuer) and “aud”(audience) claims. When encryption is applied, it can be done with or without prior signing, following the Nested JWT format (if both are used).

3.4. Registration flow

The registration flow is represented in Fig. 3. This sequence of actions starts with the user login request in an institutional service. Then, this service redirects the user to the ELIXIR node where it is necessary to choose the institution responsible for authenticating the user. In the institutional IdP, the user provides the credentials. ELIXIR will detect this as a new user, which will require the user’s consent to use personal data. At this stage, the user can choose which attributes are passed to the service via ELIXIR. Usually, these attributes are not sensitive and are provided by the institutional IdP. After this stage, the service asks for additional attributes, if necessary, to complete the registration. The service stores a registration token, which is a token provided by ELIXIR linked to the user.

After completing the registration, the user undergoes an approval process managed by a designated authority in this context. During this phase, the user’s role within the service is established, along with a tailored set of permissions that dictate their level of access and functionality within the system. This part of the flow was omitted in the figure since each service may have unique criteria for different roles.

3.5. Authentication flow

The authentication flow is similar to that of registration. Fig. 4 represents the interaction between the four entities aiming to authenticate a user to access a service. Some services require manual approval from the application manager. In these cases, users are on a waiting list until being approved, and they are blocked from using that service until their status is changed.

After successfully performing the login in one service, the user’s cookie is stored in the browser. Then, if the user tries to access another service for which there is no registration yet, the cookie will not be valid. In this case, the registration flow occurs. However, if there is already a registration in this second service, the login stage should be skipped.

4. Results and discussion

The proposed architecture aimed to fill the needs of a European project. For this reason, some decisions were limited to the European tools, namely ELIXIR AAI. In this section, we describe the use case and the implementation issues faced.

4.1. Use case

EHDEN[2] was launched in 2018 to address challenges in generating insights and evidence from real-world clinical data on a large scale. The goal of this project was to support patients, clinicians, payers, regulators, governments and industry in understanding well-being, disease, treatments, outcomes and new therapeutics and devices. To accomplish this, EHDEN aims to collaborate with several institutions, data sources and data custodians across Europe.

One of the goals of this project is to harmonize health databases into a common data model locally, within a federated network. This was addressed with the support of SMEs that work directly with the partners that have health databases. Access to these data is very restricted, and data analysis is performed using the tools defined within the project. Additionally, the project includes academic partners that aim to provide intellectual resources, new members and management tools, among others.

The ecosystem of tools is available within the EHDEN Portal,[3] which is a centralized platform for accessing all these tools [26–28]. The authentication issue described in this work was motivated by this problem, where the user needed to have credentials to log into the Portal and a set of credentials to access the remaining tools available within the Portal.

4.2. Implementation and issues

The proposed architecture was adopted and implemented in this Portal. The effort in integrating this federated mechanism was reduced, due to the OAuth 2.0 protocol. Since almost every tool already supported this protocol, the implementation effort was mainly related to the configuration of each tool. For instance, in the proposed use case, we defined the client ID, the secret key, and the three required ELIXIR AAI endpoints to establish this integration in one of our services. These endpoints are used to process the authentication and registration operations. One of these endpoints is responsible for requesting the authentication tokens. Another is responsible for gathering the user's information, and the last is for processing the authorization redirect response.

As we previously presented, the development of a federated identity manager may raise some technical challenges that can be addressed by one of the three major protocols used for it: OIDC, SAML, and OAuth 2.0 [29]. Although in the presented use case all tools supported OAuth 2.0, we recognized that the protocols SAML and OIDC could be used as well since ELIXIR AAI supports these. Therefore, the integration of this architecture is not limited to a specific protocol.

The system can transmit information between parties using a compact and self-contained mechanism when considering the use of OIDC with JWT tokens. The JSON-based format is easy to parse and use in various web environments. Moreover, JWT supports digital signatures and optional encryption, ensuring the integrity and security of the data it contains. This enables the verification of the authenticity of the token, preventing tampering or other cyber threats associated with access-control mechanisms.

The tools that did not support any of the three major protocols needed to be patched. However, solving this problem without this protocol could be too complex. Another possible issue is the dependency on ELIXIR as the central point for authentication. Currently, we rely on one ELIXIR Node, but we can have redundancy, which ensures that the infrastructure for login in the application is always up.

4.3. Evaluation

A key component of the proposed architecture is the robust validation process when registering on the platform. This process extends beyond mere digital verification, requiring a thorough verification of official personal documents. In specific scenarios, it may also require in-person validation by institutional representatives which significantly increases the confidence of all interested parties. We identify the following advantages: i) it enhances confidentiality by ensuring that sensitive information is accessible only to authenticated users; ii) it improves integrity by safeguarding against unauthorized data modifications; and iii) it boosts availability, guaranteeing reliable and consistent access to authorized users.

The foremost property is confidentiality, to secure from unapproved exposure sensitive information such as medical data. The implemented authentication mechanisms can protect this information against illicit user entry. Centralizing RBAC policies reduces the risk of misconfigurations in different environments. This centralization establishes a more reliable and secure authentication chain, ensuring that access to sensitive health information is only granted to verified users.

Data integrity is a key aspect of healthcare. In the presented use case, there is a group of users responsible for populating the system with data that characterizes health databases. This information is used by medical researchers to define the studies' feasibility before accessing the data. The authentication mechanism ensures that the data are published and verified but trustworthy users, normally the data custodians and the community manager.

[2] https://www.ehden.eu.
[3] https://portal.ehden.eu/.

The third property can be analyzed from different perspectives. Centralizing the authentication mechanisms into an AAI provider creates a new dependency on a third-party service. In case of malfunctioning, all the authentication operations will be compromised. However, in this case, the ELIXIR AAI provider has redundant nodes to ensure its continuous availability.

After the first release of the EHDEN Portal, we created a user survey to assess its overall functionalities and if they fit the initial requirements. One of the sections inquires about the authentication mechanisms, a topic deeply discussed among the project participants aiming to ensure that each user does not need distinct accounts in each of the tools that are part of the portal. From the feedback collected in this evaluation, more than 70% of the users have expressed high or much high satisfaction with the adoption of these mechanisms, *i.e.*, using a centralized SSO service that is capable of recognizing the institutional credentials. A smaller percentage of users, approximately 10% raised some concerns about the dependency of the system on a third-party service. A few participants from pharmaceutical companies expressed some reluctance about relying on external authentication services. In those cases, *i.e.*, when companies or institutions are not associated with the centralized AAI service, users need to register individually. One notable observation from the free-text responses was that the proposed mechanisms were perceived to be beneficial when used in research contexts where the partners were institutions recognized by the ELIXIR AAI. Furthermore, the answers collected also suggest that the proposed mechanism has a significant impact when it is used in research contexts.

5. Conclusion

The proposed architecture aims to provide federated identity management for healthcare projects involving multiple institutions with distinct access control policies. This work aimed to provide a solution to a problem regarding who would be responsible for authenticating and authorizing the users of the ecosystem. Since several institutions provide resources or services to the project, each one having its login services, providing an SSO mechanism on top of all these services is a key aspect. Our solution relies on an authorization and authentication infrastructure that was developed for bioinformatics projects in Europe. However, this concept can be applied in other use cases.

The proposed architecture was implemented in the authentication mechanisms of the EHDEN Portal, which is the central hub for a European project involving the collaboration of several SMEs, data partners, pharmaceutical institutions and academia from different European countries, effectively solving the problem described for this scenario. By adopting this architectural design, several advantages can be identified for the different stakeholders involved in these projects. Our proposal for authentication management facilitates communication between different IdPs. This model enforces security, simplifies the authentication process across multiple platforms, and delivers a superior user experience.

CRediT authorship contribution statement

João Rafael Almeida: Writing – review & editing, Writing – original draft, Methodology, Conceptualization. **André Zúquete:** Writing – review & editing, Writing – original draft, Supervision. **Alejandro Pazos:** Writing – review & editing, Supervision. **José Luís Oliveira:** Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

JRA is funded by the National Science Foundation (FCT), under the grant SFRH/BD/147837/2019. The EHDEN project has received funding from the Innovative Medicines Initiative 2 Joint Undertaking (JU) under grant agreement No. 806968 (supported by the European Union and EFPIA).

References

[1] Y. Wilson, A. Hingnikar, Single sign-on, in: Solving Identity Management in Modern Applications, Springer, 2019, pp. 151–157.
[2] J. Hu, Q. Sun, H. Chen, Application of single sign-on (SSO) in digital campus, in: 2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT), IEEE, 2010, pp. 725–727.
[3] S.K. Bhosale, Architecture of a Single Sign on (SSO) for Internet Banking, 2008.
[4] V. Radha, D.H. Reddy, A survey on single sign-on techniques, Proc. Technol. 4 (2012) 134–139.
[5] A. Armando, R. Carbone, L. Compagna, J. Cuellar, L. Tobarra, Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for Google apps, in: Proceedings of the 6th ACM Workshop on Formal Methods in Security Engineering, 2008, pp. 1–10.
[6] P. Pandey, T. Nisha, Challenges in single sign-on, J. Phys. Conf. Ser. 1964 (2021) 042016, https://doi.org/10.1088/1742-6596/1964/4/042016, IOP Publishing.
[7] H. Tabrizchi, M. Kuchaki Rafsanjani, A survey on security challenges in cloud computing: issues, threats, and solutions, J. Supercomput. 76 (2020) 9493–9532.

[8] M. Ates, J. Fayolle, C. Gravier, J. Lardon, Complex federation architectures: stakes, tricks & issues, in: Proceedings of the 5th International Conference on Soft Computing as Transdisciplinary Science and Technology, 2008, pp. 152–157.
[9] R. Weingärtner, C.M. Westphall, Enhancing privacy on identity providers, in: SECURWARE 2014, 93, 2014.
[10] J. Carretero, G. Izquierdo-Moreno, M. Vasile-Cabezas, J. Garcia-Blas, Federated identity architecture of the European eID system, IEEE Access 6 (2018) 75302–75326.
[11] D.W. Chadwick, Federated identity management, in: Foundations of Security Analysis and Design V, Springer, 2009, pp. 96–120.
[12] S. Cantor, J. Moreh, R. Philpott, E. Maler, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, 2005.
[13] D. Hardt, et al., The OAuth 2.0 Authorization Framework, 2012.
[14] N. Sakimura, J. Bradley, M. Jones, B. De Medeiros, C. Mortimore, Openid Connect Core 1.0, The OpenID Foundation, 2014, p. S3.
[15] N. Naik, P. Jenkins, Securing digital identities in the cloud by selecting an apposite federated identity management from SAML, OAuth and OpenID connect, in: 2017 11th International Conference on Research Challenges in Information Science (RCIS), IEEE, 2017, pp. 163–174.
[16] J. Hughes, E. Maler, Security assertion markup language (SAML) v2.0 technical overview, OASIS SSTC Working Draft 13, 2005.
[17] H. Halpin, B. Cook, Federated identity as capabilities, in: Annual Privacy Forum, Springer, 2012, pp. 125–139.
[18] A. Alonso, A. Pozo, J. Choque, G. Bueno, J. Salvachúa, L. Diez, J. Marín, P.L.C. Alonso, An identity framework for providing access to FIWARE OAuth 2.0-based services according to the eIDAS European regulation, IEEE Access 7 (2019) 88435–88449.
[19] D. Fett, R. Küsters, G. Schmitz, A comprehensive formal security analysis of OAuth 2.0, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 1204–1215.
[20] M. Linden, M. Procházka, I. Lappalainen, D. Bucik, P. Vyskocil, M. Kuba, S. Silén, P. Belmann, A. Sczyrba, S. Newhouse, et al., Common elixir service for researcher authentication and authorisation, in: F1000Research 7, 2018.
[21] M.D. Wilkinson, M. Dumontier, I.J. Aalbersberg, G. Appleton, M. Axton, A. Baak, N. Blomberg, J. Boiten, L. da Silva Santos, P. Bourne, et al., The FAIR guiding principles for scientific data management and stewardship, Sci. Data 3 (2016) 160018.
[22] L. Eijssen, C. Evelo, R. Kok, B. Mons, R. Hooft, et al., The Dutch techcentre for life sciences: enabling data-intensive life science research in the Netherlands, in: F1000Research 4, 2015.
[23] K.M. Tekle, S. Gundersen, K. Klepper, L.A. Bongo, I.A. Raknes, X. Li, W. Zhang, C. Andreetta, T.D. Mulugeta, M. Kalaš, et al., Norwegian e-infrastructure for life sciences (NeLS), in: F1000Research 7, 2018.
[24] V. Baillie Gerritsen, P.M. Palagi, C. Durinx, Bioinformatics on a national scale: an example from Switzerland, Brief. Bioinform. 20 (2019) 361–369.
[25] J. Harrow, R. Drysdale, A. Smith, S. Repo, J. Lanfear, N. Blomberg, ELIXIR: providing a sustainable infrastructure for life science data at European scale, Bioinformatics 37 (2021) 2506–2511.
[26] J.R. Almeida, A. Pazos, J.L. Oliveira, Clinical data integration strategies for multicenter studies, in: Doctoral Conference on Computing, Electrical and Industrial Systems, Springer, 2023, pp. 175–190.
[27] J.R. Almeida, J.M. Silva, J.L. Oliveira, A FAIR approach to real-world health data management and analysis, in: 2023 IEEE 36th International Symposium on Computer-Based Medical Systems (CBMS), IEEE, 2023, pp. 892–897.
[28] J.R. Almeida, J.L. Oliveira, MONTRA2: a web platform for profiling distributed databases in the health domain, Inform. Med. Unlocked 45 (2024) 101447.
[29] S. Koussa, Federated identities: openid vs. SAML vs. OAuth, http://www.softwaresecured, http://www.com/2013/07/16/federated-identities-openid-vs-saml-vs-oauth/, 2013 (cit. 25.04.2016).