Integration of an Open Source Identity Management System in Educational Platforms

Enrique Barra[1,*], Alejandro Pozo[1], Sonsoles López-Pernas[2], Alvaro Alonso[1] and Aldo Gordillo[1]

[1] *Universidad Politécnica de Madrid, Madrid, 28040, Spain*
[2] *University of Eastern Finland, Joensuu, 80100, Finland*
E-mail: enrique.barra@upm.es; alejandro.pozo@upm.es; sonsoles.lopez@uef.fi; alvaro.alonso@upm.es; a.gordillo@upm.es
[*] *Corresponding Author*

Received 29 January 2024; Accepted 05 July 2024

Abstract

Making research advances available to the community in the shape of open source software has the potential to introduce cutting-edge innovations from early on, foster collaborative development, and revolutionize industrial applications. However, including open source software resulting from a research project as part of a production system poses some risks and must be evaluated in detail, considering all pros and cons. This is especially delicate when that piece of software is in charge of authentication and authorization. This article reports on an experience of integrating open source identity and access management (IAM) software that is the result of multiple research projects, the FIWARE Keyrock IAM, into three educational web-based platforms: two learning object repositories and a course management platform. We intend to draw the lessons learned from this experience so they can guide software practitioners when deciding if they should integrate open source software developed in research projects.

Keywords: Identity and access management, software integration, single sign on, educational platforms.

Journal of Web Engineering, Vol. 23_4, 595–610.
doi: 10.13052/jwe1540-9589.2345

1 Introduction

Identity and access management (IAM) is one of the keyrocks in the software industry. IAM solutions enable organizations to safeguard data, ensure regulatory compliance and deliver a streamlined and improved user experience. These solutions are tailored to protect organization assets by granting access to specific data and resources only to authorized individuals and under appropriate conditions. These qualities make IAM systems an attractive niche for academia due to the wide variety of research lines (e.g., protocols or privacy issues), but also for industry, as the IAM system is a central piece of almost every large software project, especially when the final product or service is composed of multiple systems that the user has to access with the same identity and, hence, single sign on (SSO) capabilities become a necessity.

Organizations such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), and the Organization for the Advancement of Structured Information Standards (OASIS) promote the creation of discussion spaces to create open standards and define features related to IAM technology in which any individual can participate and where academia and industry can confluence. As a result, they have developed and published widely used standards such as OAuth 2.0, SAML2, and Verifiable Credentials, which establish some basis for the research and development of IAM systems [1]. Thanks to the implementation of these standards, IAM systems can be deployed as independent components where services and applications delegate the authentication and authorization processes.

One possibility to select the IAM system for a project is to choose a proprietary product like the ones provided by big companies and organizations such as IBM, Sun, Oracle, or Novell [2]. The other possibility is to make use of open source components such as Keycloack, Gluu, Shibboleth, OpenIAM, and FreeIPA, among others. Some of these open source components are also results of research projects or are continuously enhanced (developing new experimental features or functionalities) as part of research projects.

The project framework and context usually impose certain conditions that limit the possibilities when choosing the IAM system to integrate or use. On the one hand, is the project budget which, if tight, will exclude the most expensive solutions. On the other hand, we can find functional and non-functional requirements defined by the client that will also reduce the number of possible alternatives, a clear example of this is the need for compatibility with established systems involved in the project that only support some authentication methods.

At Universidad Politécnica de Madrid, we were tasked to integrate a learning management system (LMS) within three different educational software platforms using single sign-on: two learning object repositories and a course management platform. In other words, we were required to seamlessly connect each of the systems with their corresponding LMS as though they were one. In this article, we describe how we used the FIWARE IAM system, experimental open-source software, to manage the seamless authentication and authorization of the users. The next section describes the FIWARE IAM system, Keyrock Identity Manager. Next, we describe the three educational projects and how the integration was achieved. Lastly, the last section outlines the main lessons learned.

2 FIWARE Keyrock

The FIWARE European project (https://www.fiware.org) was funded in 2011 under the Seventh Framework Programme (FP7) for Research and Innovation. It aimed to provide an open source framework for developing smart applications for the future internet. This project was followed by other related research projects and in 2016 the FIWARE Foundation was created with the objective of building a sustainable community around FIWARE.

FIWARE is based on a service ecosystem composed of key elements called generic enablers (GEs), which encompass a framework that allows the development of smart applications relying on smart services and data management components. Keyrock is one of these GEs.

Keyrock (https://keyrock-fiware.github.io) is an open source component and part of the FIWARE security catalog. Keyrock is responsible for identity and access management. The basic Keyrock usage enables OAuth 2.0-based authentication and authorization security for services and applications. Keyrock also offers a two-factor authentication (2FA) mechanism so that users can use their smartphones in conjunction with the username/password mechanism to enforce the authentication process. The 2FA mechanism is based on RFC 4226, "HOTP: An HMAC-Based One-Time Password Algorithm" and in RFC 6238 "TOTP: Time-Based One-Time Password Algorithm".

Keyrock can manage authorization policies and decide who can access which resources. Particularly, Keyrock enables the implementation of a role based access control (RBAC) mechanism by playing the role of PAP (policy administration point) and PDP (policy decision point). Keyrock together with another FIWARE generic enabler called Wilma (https://github.com/ging/fiware-pep-proxy) make it possible to implement a robust system that controls access to information only to users that are entitled to it by the Keyrock policy definition.

With this approach, Keyrock offers support to authentication, authorization, and access control, but it also goes beyond them offering the possibility of offering data usage control in data sharing scenarios [3].

The Keyrock features and integrations have been increased thanks to the research done in the FIWARE continuation projects or related research projects that used FIWARE as the enabling technology. Relevant examples include:

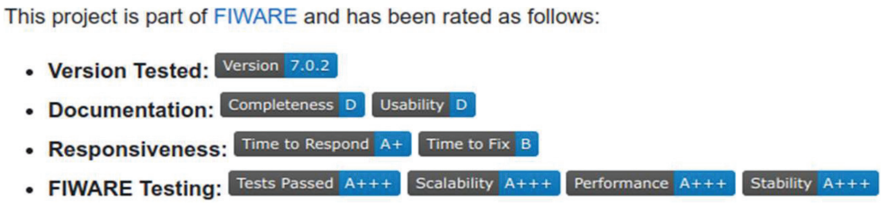
- **Electronic IDentification (eID) integration** [4]. Keyrock was one of the core elements in co-financed European projects that involved the electronic identification, authentication and trust service (eIDAS) regulation. Keyrock was extended to work as a gateway between applications and the cross-border eIDAS infrastructure based on eID authentication. Keyrock was also extended to support the eID attributes as well as a new set of academic attributes defined during the projects.
- **Accessibility** [5]. Keyrock was extended to support functional attributes regarding vision, cognition, hearing, etc. Keyrock was able to obtain these attributes by externally certified entities and by the use of the aforementioned eID model.
- **Industrial data spaces (IDS) reference architecture model implementation** [6]. The IDS framework seeks to create a common frame to design and deploy the industry 4.0 infrastructure fulfilling trust, governance, and sovereignty requirements. Keyrock was presented to implement a part of these security requirements.
- **Data usage control** [3, 7]. In terms of data exchange and security, in addition to controlling who can access which resource, it is also important to control how data is allowed to be used. Keyrock was integrated into an architecture that enabled the application of usage control policies and was extended to support the definition of this type of architecture.
- **Internet of Things (IoT)** [8]. Security is one of the main concerns regarding research on IoT. In a research line about the protection of IoT devices that communicate using a publish/subscribe pattern, Keyrock was extended to support the OAuth 2.0 protocol over a different application protocol to the one defined by the standard.

Keyrock is available as an open source software project so anyone can contribute to the codebase with any new feature, bug fixing, and modification. Contributions to the project have been made by FIWARE Foundation engineers, university partners through shared research projects and, less often, by third parties. All contributions must satisfy a set of obligations imposed by FIWARE which serve as a bridge between the results of the research conducted and the industry companies and projects that rely on them.

These obligations are a set of actions over the software to guarantee the tool's performance, reduce security risks, or maintain the code clean, among others. Relevant obligations include:

- **Testing**. All contributions and commits to the repository must run a set of unit and integration tests to check if the code changes break down the normal functioning. The code coverage of the tests is also measured.
- **Security**. Keyrock is a Node.js-based software that relies on several dependencies. It also relies on specific software that seeks known vulnerabilities in the different dependencies versions and notifies the maintainers to act over them. Keyrock has also obtained a security best practices certification granted by OpenSSF (Open Source Security Foundation).
- **Releasing**. FIWARE proposes a release calendar to create stable versions. It makes it easier for developers to use Keyrock, manage changes in the code, and migrate databases.
- **Deployment**. Keyrock is dockerized so it can be installed by deploying containers. Keyrock provides distroless images which are light containers that boost deployments. It also provides guidelines to be directly deployed by cloning the repository and installing its dependencies (database and email server) together.
- **Documentation and tutorials**. Documentation plays an important role for open source software. FIWARE demands Keyrock to have a readable README, roadmap, and API description. It also demands a "Readthedocs" repository with all the usage and configuration descriptions in the different releases, as well as a set of tutorials.
- **Code styling and quality**. FIWARE also requires a linter to be installed to control the style and structure of the code. The linter defines a set of rules that must be followed by any contribution to Keyrock. Thus, any changes must be in accordance with these rules. Keyrock tracks the code quality using Codacy tool. Currently, Keyrock has a grade A, which is the maximum grade in Codacy.

FIWARE also proposes a quality assurance (QA) mechanism for the GEs where several parameters are rated following a simple but meaningful



This project is part of FIWARE and has been rated as follows:

- **Version Tested:** Version 7.0.2
- **Documentation:** Completeness D Usability D
- **Responsiveness:** Time to Respond A+ Time to Fix B
- **FIWARE Testing:** Tests Passed A+++ Scalability A+++ Performance A+++ Stability A+++

Figure 1 FIWARE Keyrock QA rating.

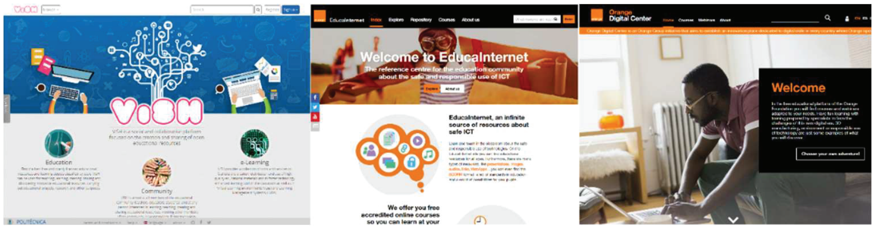

ViSH
Welcome to EducaInternet
The reference centre for the education community about the safe and responsible use of ICT
EducaInternet, an infinite source of resources about safe ICT
We offer you free accredited online courses so you can learn at your
Orange Digital Center
Welcome

Figure 2 Front pages of ViSH, EducaInternet, and Orange Digital Center.

labeling schema, the energy labeling system applied by the European Union for devices, applying the labels A+++, A++, A+, A, B, C, D, E, F, or G according to the rating obtained, where A+++ is the highest and G the lowest. The ratings for the Keyrock GE can be seen in Figure 1.

3 Integration in Three Educational Platforms

The three educational platforms where we have integrated the FIWARE Keyrock can be seen in Figure 2. The first one is Virtual Science Hub (ViSH), an enriched learning object repository (LOR) focused on the creation, sharing, and distribution of learning resources and educational activities [9]. Its codebase is open source, and it is deployed in production at https://vishub.org. This service is offered by the Universidad Politécnica de Madrid (UPM) and is open to the entire educational community. The second one is EducaInternet, a learning object repository about the safe and responsible use of ICT [10]. It is also open source and deployed in production at https://educainternet.es and https://educainternet.org. Finally, the Orange Digital Center is a course and webinar management platform. It is also open source and deployed in production at https://online.orangedigitalcenter.es. Both the EducaInternet platform and the Orange Digital Center are services offered by the Orange Foundation in Spain, open to the educational community as a whole.

In the ViSH and EducaInternet platforms, the use case consisted of enhancing the system by adding learning management system (LMS) capabilities to be able to deliver courses using the learning resources stored in the platforms. In the case of Orange Digital Center, the LMS was in the initial requirements as one of its main features is offering online courses and conducting them. Therefore, the challenge was to seamlessly connect each platform with the LMS using SSO techniques. We chose Moodle as the LMS in all three cases. In the educational sector, Moodle is one of the most used LMSs [11] because it is open source, well documented, and has many features and functionalities that make it a good choice for conducting almost any kind of course. Moodle supports the following SSO technologies without having to install any additional plugins: CAS, LDAP, Shibboleth, and OAuth 2.0.

All three cases described above had a reduced budget to carry out the installations, deployments, and essential developments. This made us choose an open-source solution for the IAM system that we could install and customize. The main functional requirement that the component should meet was to support at least one of the authentication methods supported by Moodle. Another important requirement was to support localization, as all three platforms utilized both the Spanish and English languages.

We chose FIWARE's Keyrock Identity Manager since it is open source and its specifications met the main functional requirements needed, supporting OAuth 2.0 and localization. Keyrock also provides secondary functionalities such as 2FA or policy definition and enforcement that users and administrators may find useful to integrate into educational platforms. These functionalities contribute to make a more robust security system in terms of authentication, authorization, and access control. Additionally, it met other non-functional requirements that made it the best candidate. It is a long-term project in which FIWARE imposes certain obligations and quality assurance for the software; as discussed in the previous section the code is structured following the model-view-controller (MVC) pattern and therefore it is easily modifiable, and the Keyrock development team was active and supportive and encouraged us to contribute to the project.

We have also chosen FIWARE's Keyrock Identity Manager as a forward-looking solution for grades and courses digital certification. Keyrock includes on its roadmap the integration with the European Blockchain Service Infrastructure (EBSI) which may enable the emission and validation of verifiable credentials. The EBSI platform provides a trusted and decentralized way to generate traceable and transparent education certificates that will automate many verification processes.

Four developments were needed to adapt Keyrock to our use cases. The most important change was adding compatibility with an existing user database. Keyrock was designed to be included in new projects but was not ready to be added to projects in production with active users already registered in its own database, such as ViSH and EducaInternet. The other possibility would have been to migrate these user databases to Keyrock and modify the code of ViSH and EducaInternet to connect to these new databases to retrieve user data, but they are older projects that are more difficult to modify, so we opted for the first option. Moreover, by developing this feature we could also contribute to Keyrock's codebase.

Another feature that we developed within Keyrock was the possibility of skipping the authorization consent screen, a prompt that tells users who's requesting access to their data and what kind of data users are allowing the application to access. In our three cases, the integration was among the Moodle LMS and the platform "landing page" and thus that consent was explicit when registering in the service as it appeared in the terms of use. To skip that consent screen, we added an additional option "ask_authorization" (that defaults to true) in the configuration file and modified the code to skip that screen if the option was set to false.

We also added a single sign out feature. This is a characteristic that is not present in the OAuth 2.0 standard but in our use case, it was necessary since a requirement was that if a user exits the educational platform, he/she should also logout from Moodle and vice versa. To achieve this, we added an API endpoint to make an Ajax request and after validation of this request, a logout was performed in Keyrock.

Finally, the last adaptation was to create a specific CSS theme to show a login page similar to the user interface of each of the platforms where it was going to be integrated. For this, we had to create three themes, one for each platform.

4 Results

We encountered several problems when integrating Keyrock. As Keyrock was developed in the framework of multiple research projects, less attention is paid to industry-required tasks such as deployment, scalability, and maintainability (which can be also considered non-functional requirements for a project). Regarding deployment, Keyrock encourages deployment using docker images, but we were forced to do it directly from the project's repository because we had modified the code to connect to our existing database and also we wanted to use our production email service to communicate with the users (registration email, password recovery email and so on). The deployment instructions were very straightforward, and we had to investigate how to do a more advanced deployment. With respect to scalability, we were not able to find any description of the supported load and performance or any additional documentation. We used PM2 (a production process manager for Node.js applications with a built-in load balancer) to monitor the process and be able to scale in the future if needed. With respect to maintainability, Keyrock is actively maintained by the FIWARE Foundation and the community formed around it, but we had to dedicate additional efforts to discerning whether the new versions include changes that we need or if they break functionalities that we use. Furthermore, there was no version migration guide.

One very positive aspect of integrating an active open source component into our systems was that it opens new possibilities for participating in funded research projects that require a research partner that is well-versed in said project. In our case, the ViSH platform was one of the three services that participated in the CEF eID4U project (https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2017-eu-ia-0051). This project proposed an extension of the user profile attributes (such as name, surname, birth date, etc.) retrieved from the eID authentication through the eIDAS network. The extension consisted of academic attributes (such as academic degrees, grades, English level, etc.) retrieved from an external organization attribute provider (AP) service. This functionality was added to Keyrock during the project and after the integration citizens of any European country could use their national eIDs to securely access ViSH and also their profile was automatically filled in with their personal information (e.g., name, birthdate, gender, etc.) – if they allowed it in the registration process [12, 13]. Surveyed users perceived positively the eID integration with Moodle and the Vish Platform [13].

We can confidently say this integration has been a success story since it was done in late 2018 and it is still being used in production in EducaInternet with more than 5,000 registered users and in the Orange Digital Center with more than 21,000 registered users.

In the ViSH platform, which has more than 3,500 registered users, it was used for 4 years but the Moodle service was not being used so it was removed recently together with the SSO mechanism, keeping a local authentication against its database.

5 Lessons Learned

We hope that our experience can be useful to other organizations when deciding whether to integrate a research-oriented open source component into their system. We have described the process we followed and outlined the works that had to be done but we would like to finish with some lessons learned and pieces of advice that might be useful in the decision process and during the project lifecycle.

- When looking for a suitable open source component there are many alternatives, and a first quick filtering process has to be done by discarding discontinued or low rated projects (based for example on GitHub stars or reviews in Sourceforge) and those that do not fit the project functional or non-functional requirements (in our case the system had to support an authentication method among the ones included in Moodle and localization). When there are just a few alternatives remaining, other factors should influence the decision, such as good code structure and documentation, having an active community, and using any kind of quality assurance (QA) mechanism [14]. These factors can be analyzed by reviewing comparisons in specialized forums and blogs or directly with the information described on the project homepage. In our case, the support of the FIWARE foundation to Keyrock gave us the required confidence. Keyrock was a long-term project and followed a well-defined QA process and a minimum set of obligations to make the software ready for production.
- One part of the QA process will be to adhere to a software versioning scheme and keep it. But in research projects, it is typical to release major versions that include new experimental functionalities (results of the research project or part of it) along with bug fixes and to abandon the earlier versions hastily (because it is expensive to continue to support them). Thus, it is necessary to carefully check the new version changes and see if there is any breaking change in the functionalities being used. Furthermore, the migration guide is not usually very well detailed or is directly nonexistent as the interest of the research project is to promote the new experimental features and not take care of those with older versions. The counterpart of this is that it includes new features resulting from research projects that can be very interesting and that almost no other software has, and that can make a big difference with other systems. It is advisable to keep an eye on the research projects in which the software is used.

- Related to this last point, if the open source component is actively being modified or enhanced within a research project, it is recommended to be in contact with the development team to make them aware of your use of the software and your interest in participating in funded research projects. This can generate interesting opportunities for extending the use of your system and improving it.

Acknowledgement

The authors would like to acknowledge the support of the FUN4DATE (PID2022-136684OB-C22) project funded by the Spanish Agencia Estatal de Investigacion (AEI) 10.13039/501100011033.

Funding Statement

This work was funded by the Spanish Agencia Estatal de Investigacion (AEI) 10.13039/501100011033 with the project FUN4DATE (PID2022-136684OB-C22).

Author Contributions

The authors confirm contribution to the paper as follows: study conception and design: E. Barra, A. Pozo; data collection: E. Barra; analysis and interpretation of results: A. Alonso, A. Gordillo; draft manuscript preparation: E. Barra, A. Pozo, S. López-Pernas. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials

The software projects used in this study are open source and available at GitHub platform. https://github.com/FIWARE-GEs/keyrock, https://github.com/ging/vish_orange and https://github.com/ging/vish.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Pohn D, Hommel W (2023) New Directions and Challenges within Identity and Access Management. IEEE Communications Standards Magazine 7:84–90. https://doi.org/10.1109/MCOMSTD.0006.2200077.

[2] Kumar V, Bhardwaj A (1AD) Identity Management Systems: A Comparative Analysis. International Journal of Strategic Decision Sciences 9:63–78. https://doi.org/10.4018/IJSDS.2018010105.

[3] Munoz-Arcentales A, López-Pernas S, Pozo A, Alonso Á, Salvachúa J, Huecas G (2020) Data Usage and Access Control in Industrial Data Spaces: Implementation Using FIWARE. Sustainability 2020, Vol. 12, Page 3885 12:3885. https://doi.org/10.3390/SU12093885.

[4] Alonso A, Pozo A, Choque J, Bueno G, Salvachua J, Diez L, Marin J, Alonso PLC (2019) An Identity Framework for Providing Access to FIWARE OAuth 2.0-Based Services According to the eIDAS European Regulation. IEEE Access 7:88435–88449. https://doi.org/10.1109/ACCESS.2019.2926556.

[5] Marco L, Pozo A, Huecas G, Quemada J, Alonso Á, Gil D, Luján-Mora S, Medina Quero J, Espinilla-Estévez M (2021) User-Adapted Web Services by Extending the eIDAS Specification with Functional Attributes. International Journal of Environmental Research and Public Health 2021, Vol. 18, Page 3980 18:3980. https://doi.org/10.3390/IJERPH18083980.

[6] Alonso Á, Pozo A, Cantera JM, de la Vega F, Hierro JJ (2018) Industrial Data Space Architecture Implementation Using FIWARE. Sensors 2018, Vol 18, Page 2226 18:2226. https://doi.org/10.3390/S18072226.

[7] Munoz-Arcentales A, López-Pernas S, Pozo A, Alonso A, Salvachua J, Huecas G (2019) An Architecture for Providing Data Usage and Access Control in Data Sharing Ecosystems. Procedia Computer Science 160:590–597. https://doi.org/10.1016/J.PROCS.2019.11.042.

[8] Pozo A, Alonso Á, Salvachúa J (2020) Evaluation of an IoT Application-Scoped Access Control Model over a Publish/Subscribe Architecture Based on FIWARE. Sensors 2020, Vol. 20, Page 4341 20:4341. https://doi.org/10.3390/S20154341.

[9] Barra E, Gordillo A, Quemada J (2014) Virtual Science Hub: An Open Source Platform To Enrich Science Teaching. In: International Conference on Educational Sciences and Technology. pp. 741–746.

[10] Barra E, Gordillo A, Blas ME, Guijarro J, Vazquez I (2015) EducaInternet: A Platform to Teach and Learn Safe and Responsible Use of

Digital Technologies. Proceedings of the 8th International Conference of Education, Research and Innovation (ICERI).

[11] Karadimas N V. (2018) Comparing Learning Management Systems from Popularity Point of View. Proceedings - 2018 5th International Conference on Mathematics and Computers in Sciences and Industry, MCSI 2018 141–146. https://doi.org/10.1109/MCSI.2018.00040.

[12] Alonso González Á, Gordillo Méndez A, Pozo Huertas A, López Pernas S, Marcos Pascual L, Barra Arias E (2019) Extending the EIDAS European Specification for Supporting Academic Attributes. In: 12th annual International Conference of Education, Research and Innovation (ICERI 2019). E.T.S.I. Telecomunicación (UPM), pp. 2008–2014.

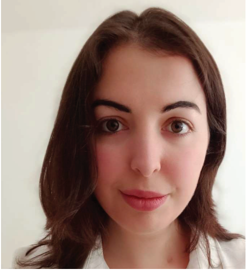
[13] Alonso Á, Pozo A, Gordillo A, López-Pernas S, Munoz-Arcentales A, Marco L, Barra E (2020) Enhancing university services by extending the eIDAS European specification with academic attributes. Sustainability 12: https://doi.org/10.3390/SU12030770.

[14] Aberdour M (2007) Achieving quality in open-source software. IEEE Software 24:58–64. https://doi.org/10.1109/MS.2007.2.

Biographies

Enrique Barra is an Associate Professor at Universidad Politécnica de Madrid. His research interests include the generation and distribution of educational content, games, and social networks in education. He received his Ph.D. in Engineering from Universidad Politécnica de Madrid.

Alejandro Pozo is an Assistant Professor at Universidad Politécnica de Madrid. His research interests include data engineering and cybersecurity. He received his Ph.D. in Engineering from Universidad Politécnica de Madrid.



Sonsoles López-Pernas is a Senior Researcher at University of Eastern Finland. Her research interests include educational escape rooms and learning analytics. She received her Ph.D. in Engineering from Universidad Politécnica de Madrid.

Álvaro Alonso is an Associate Professor at Universidad Politécnica de Madrid. His research interests include multi-videoconferencing systems, security management in smart context scenarios and public open data.

Aldo Gordillo is an Associate Professor at Universidad Politécnica de Madrid. His research interests include game-based learning and educational technology. He received his Ph.D. in Telematics Engineering from Universidad Politécnica de Madrid.